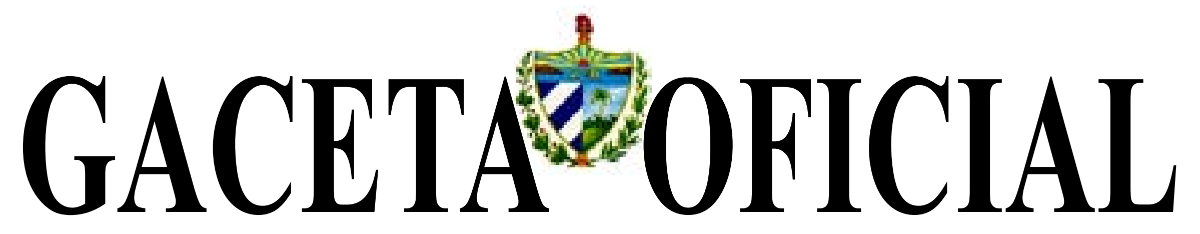
ISSN 1682-7511



DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

Información en este número

Gaceta Oficial No. 45 Ordinaria de 4 de julio de 2019

ISSN 1682-7511



DE LA REPÚBLICA DE CUBA

MINISTERIO DE JUSTICIA

EDICIÓN ORDINARIA LA HABANA, JUEVES 4 DE JULIO DE 2019 AÑO CXVII

Sitio Web: http://www.gacetaoficial.gob.cu/—Calle Zanja No. 352 esquina a Escobar, Centro Habana

Teléfonos: 7878-4435 y 7870-0576

Número 45 Página 763

CONSEJO DE ESTADO

GOC-2019-547-O45

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente del Consejo de Estado de la República de Cuba.

HAGO SABER: Que el Consejo de Estado ha considerado lo siguiente:

POR CUANTO: La informatización de la sociedad en Cuba desempeña un papel significativo en el desarrollo político, económico y social del país y constituye un medio efectivo para la consolidación de las conquistas del Socialismo y el bienestar de la población.

POR CUANTO: Resulta de interés del Estado cubano elevar la soberanía tecnológica, en beneficio de la sociedad, la economía, la seguridad y defensa nacional; contrarrestar las agresiones cibernéticas; salvaguardar los principios de seguridad de nuestras redes y servicios; así como defender los logros alcanzados por nuestro Estado Socialista, siendo necesario emitir la norma jurídica que regule la informatización de la sociedad en Cuba.

POR TANTO: El Consejo de Estado en el ejercicio de las atribuciones que le han sido conferidas en el inciso c), del Artículo 90 de la Constitución de la República de Cuba, adopta el siguiente:

DECRETO-LEY No. 370
"SOBRE LA INFORMATIZACIÓN DE LA SOCIEDAD EN CUBA"
TÍTULO I
OBJETO, OBJETIVOS, ORGANIZACIÓN INSTITUCIONAL, COMPETENCIA Y ATRIBUCIONES

CAPÍTULO I
OBJETO Y OBJETIVOS

Artículo 1. El Estado promueve el desarrollo y utilización de las Tecnologías de la Información y la Comunicación, con el objetivo de que constituyan una fuerza política, científica y económica, que contribuya y propicie la integración y conducción de los procesos asociados a la informatización de la sociedad.

Artículo 2. La informatización de la sociedad es el proceso de aplicación ordenada y masiva de las Tecnologías de la Información y la Comunicación en la gestión de la

información y el conocimiento, con la seguridad requerida, para satisfacer gradualmente las necesidades de todas las esferas de la vida social, en el esfuerzo por parte del Estado de lograr cada vez más eficacia y eficiencia en los procesos, así como mayor generación de riquezas y aumento de la calidad de vida de los ciudadanos.

Artículo 3. Se denominan Tecnologías de la Información y la Comunicación, en lo adelante TIC, al conjunto de recursos, herramientas, equipos, programas y aplicaciones informáticas, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información en cualquier formato: voz, datos, texto, video e imágenes.

Artículo 4. El presente Decreto-Ley es aplicable a las relaciones jurídicas relacionadas con las TIC y tiene como objeto establecer su marco legal, de tal forma que ordene y garantice el derecho al acceso y participación de las personas naturales y jurídicas en la informatización de la sociedad, en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales, así como los tratados y demás instrumentos jurídicos internacionales en la materia, de los que la República de Cuba es Estado Parte.

Artículo 5. Los objetivos del presente Decreto-Ley son los siguientes:

a) Fortalecer el proceso de informatización, en función de modernizar coherentemente todas las esferas de la sociedad y contribuir al desarrollo económico y social del país;
b) consolidar el uso y desarrollo de las TIC, como instrumento para la defensa de la Revolución;
c) promover y favorecer el acceso y el uso responsable de los ciudadanos a las TIC;
d) consolidar la defensa política y la ciberseguridad frente a las amenazas, los ataques y riesgos de todo tipo;
e) preservar y desarrollar los recursos humanos asociados a la actividad;
f) satisfacer las necesidades generales para incrementar el uso de las TIC y su aplicación por el Estado, el Gobierno, en la Seguridad y Defensa Nacional, y el Orden Interior;
g) favorecer el uso de las TIC en los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin fines de lucro y las organizaciones políticas, sociales y de masas;
h) asegurar la sostenibilidad y soberanía tecnológica de las TIC, en función del desarrollo de la informatización del país; e
i) incentivar y promover la integración de la investigación, desarrollo e innovación con la producción y comercialización de equipos, programas y aplicaciones informáticas, contenidos y servicios asociados a las TIC.

CAPÍTULO II
ORGANIZACIÓN INSTITUCIONAL

Artículo 6. La informatización de la sociedad cubana se garantiza por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, según su misión y funciones específicas, con la contribución de las formas asociativas sin fines de lucro, y las organizaciones políticas, sociales y de masas.

Artículo 7. El Ministerio de Comunicaciones, en coordinación con los de las Fuerzas Armadas Revolucionarias y del Interior, es el responsable de orientar las tareas y acciones que garanticen la informatización de la sociedad.

CAPÍTULO III
COMPETENCIA Y ATRIBUCIONES
SECCIÓN PRIMERA
Competencia del Ministerio de Comunicaciones respecto al proceso de informatización de la sociedad

Artículo 8. El Ministerio de Comunicaciones es el organismo encargado de otorgar la autorización, entendida esta como la licencia concedida a una persona natural o jurídica en el ámbito de las TIC, para según las condiciones que en esta se establecen, proyectar, instalar, mantener y comercializar programas y aplicaciones informáticas o proveer un servicio relacionado con lo autorizado.

Artículo 9. Es competencia del Ministerio de Comunicaciones, en el proceso de informatización de la sociedad, en colaboración con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, las formas asociativas sin fines de lucro y las organizaciones políticas, sociales y de masas, de acuerdo con las prioridades económicas y sociales del país, y con su misión y funciones específicas:

a) Organizar, normar y estandarizar la actividad informática en los órganos y organismos del Estado y del Gobierno a todos los niveles que corresponda;
b) fomentar la producción de equipamiento vinculado a las TIC e incentivar su establecimiento en zonas especiales de desarrollo, en correspondencia con las prioridades de informatización del país;
c) coadyuvar al desarrollo y modernización de la infraestructura tecnológica, que permita un empleo eficiente de los recursos y garantice la seguridad, calidad y el acceso a los servicios de las TIC para toda la sociedad, así como el despliegue y desarrollo de infraestructuras tecnológicas en los sectores productivos y de servicios con impacto en la sociedad;
d) promover la integración ordenada de las redes institucionales y de uso público, en función del acceso a los servicios y que garantice su seguridad;
e) fomentar de forma racional un sistema de centros de datos con condiciones tecnológicas, respaldo y seguridad adecuados, como soporte al proceso de informatización y a las necesidades de las entidades que lo requieran;
f) potenciar el desarrollo de la infraestructura de telecomunicaciones, en especial el despliegue de la banda ancha, para garantizar su cobertura nacional y ampliar la capilaridad en la red de acceso, fundamentalmente con el empleo de tecnologías inalámbricas que incluye la móvil;
g) participar en el diseño e implementación del sistema de gestión integrada del capital humano del sector de las TIC;
h) impulsar la cooperación internacional, en función de fortalecer el desarrollo de las TIC y la participación del país en foros internacionales y multilaterales, que permitan la adopción de estándares para el desarrollo de las TIC;
i) establecer convenios y alianzas que contribuyan al desarrollo de soluciones, el acceso, las transferencias de tecnologías y el desarrollo del capital humano;
j) promover el desarrollo y la implementación de los servicios en línea entre las instituciones y hacia los ciudadanos, con prioridad en los servicios y trámites de la población, la gestión del gobierno y el comercio electrónico;
k) conducir la elaboración de los planes para el desarrollo y uso de las TIC en cada sector de la economía, con prioridad en aquellos que sean estratégicos, así como a nivel territorial;

l) apoyar el fortalecimiento de las entidades especializadas en las TIC, de manera que haya una mayor integración y mejor conducción de los procesos asociados a la informatización de la sociedad, así como crear alianzas entre las diferentes empresas y las entidades de ciencia, tecnología e innovación del país para alcanzar los objetivos estratégicos que se proponga la nación;

m) garantizar el diseño e instrumentación de un sistema que perfeccione, armonice y desarrolle el marco legal que sustente el proceso de informatización de la sociedad, así como el control y fiscalización de su cumplimiento; y

n) coadyuvar a que los procesos de informatización se desarrollen con un análisis organizacional y un enfoque sistémico integrado.

SECCIÓN SEGUNDA

Competencia de los órganos, organismos y entidades nacionales del Estado y del Gobierno en el proceso de informatización de la sociedad

Artículo 10. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de acuerdo con su misión y funciones específicas aprobadas, desarrollan las acciones que se establecen mediante el presente Decreto-Ley, en el marco del proceso de informatización de la sociedad cubana.

Artículo 11. El ministro de Comunicaciones propone al Consejo de Ministros para su aprobación, con la participación del Ministerio de Economía y Planificación, el Programa Nacional de Informatización, que integre y armonice por cada sector, y a nivel territorial, las principales prioridades del país a corto, mediano y largo plazos a los fines de su incorporación a los planes de la economía del país y una vez aprobado realiza su implementación así como establece los indicadores de dicho Programa que puedan medir su impacto.

Artículo 12. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular son los responsables de implementar en sus planes las actividades que le correspondan dentro del Programa Nacional de Informatización, y su aseguramiento económico.

TÍTULO II

DESARROLLO DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I

INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Artículo 13. Se entiende por programa y aplicación informática, conocido como software, al programa de computación o conjunto de estos, procedimientos y posible documentación y datos asociados, entre los que se encuentran:

a) Programa y aplicación informática de código abierto: es aquel que posee licencia y permite, con mayores o menores restricciones, ejecutar, modificar y distribuir la aplicación informática, brinda acceso a sus programas listados de códigos fuente, con reconocimiento o no del autor;

b) programa y aplicación informática propietario, también llamado software no libre, software privativo, software privado, software propietario o software de propiedad: es aquel en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo, con o sin modificaciones, o cuyo código fuente no está disponible o el acceso a este se encuentra restringido.

Artículo 14. El alcance de la industria de programas y aplicaciones informáticas, en lo adelante la Industria, comprende a las entidades y al trabajador por cuenta propia, cuya función, objeto social o actividad económica autorizada es el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos asociados a esta industria.

Artículo 15. El Ministerio de Comunicaciones organiza, coordina y promueve la Industria, en correspondencia con las prioridades de informatización del país, orientadas a fortalecer la soberanía tecnológica, la sustitución de importaciones y el incremento de exportaciones.

Artículo 16. Corresponde al Ministerio de Comunicaciones implementar el sistema de control administrativo de inscripción de los programas y aplicaciones informáticas y de los servicios asociados a las TIC, que se pretendan comercializar, así como sus desarrolladores.

Artículo 17. El Ministerio de Comunicaciones adopta las acciones necesarias, en coordinación con los organismos competentes, para incrementar la producción nacional y las exportaciones de programas y aplicaciones informáticas de la Industria.

Artículo 18. El Ministerio de Comunicaciones, en coordinación con los organismos competentes, y para perfeccionar los mecanismos de gestión, actualización, socialización y comercialización de servicios, contenidos digitales y dispositivos informáticos, adopta las acciones necesarias en cuanto a:

a) Establecer una plataforma nacional que incentive la generación de contenidos y garantice la posibilidad de socializarlos, dirigidos a fortalecer la identidad, el respeto y el conocimiento a la cultura e historia nacional, así como a preservar los valores de la sociedad cubana;
b) promover la ampliación de capacidades y el uso de Internet, con precios cada vez más accesibles y competitivos;
c) controlar que se establezcan modelos de negocios entre el operador de redes de telecomunicaciones y los proveedores de servicios, programas y aplicaciones informáticas, de manera que se estimule la producción de contenidos y servicios digitales nacionales; y
d) favorecer que se implemente una estrategia de precios asequible para la comercialización de los dispositivos informáticos, la producción de aplicaciones y contenidos, así como el uso racional de la infraestructura.

Artículo 19. El Ministerio del Comercio Exterior y la Inversión Extranjera, en coordinación con el de Comunicaciones, establece e implementa la estrategia para la exportación de programas y aplicaciones informáticas, servicios y contenidos digitales.

Artículo 20. Los ministerios de Cultura y de Ciencia, Tecnología y Medio Ambiente, en lo referido al derecho de autor y a la propiedad intelectual respectivamente, en coordinación con el Ministerio de Comunicaciones, establecen las normas para la protección a los autores y titulares de programas y aplicaciones informáticas, a partir de las necesidades del desarrollo científico y tecnológico del país en la explotación de este tipo de creación, así como los mecanismos que garanticen la protección del patrimonio nacional.

Artículo 21. El Ministerio de Comunicaciones, con la participación del de Economía y Planificación, establece el diseño económico que permita aumentar y diversificar las fuentes de financiamiento, en respaldo a la modernización de la infraestructura tecnológica, así como a las prioridades del Programa Nacional de Informatización.

Artículo 22. Los operadores de redes de telecomunicaciones y los proveedores de servicios TIC garantizan la oferta de tarifas preferenciales para impulsar las capacidades tecnológicas de las entidades de programas y aplicaciones y servicios informáticos; de igual manera, los suministradores de equipamiento informático establecen precios preferenciales, comparables a los internacionales, a las entidades que desarrollan programas y aplicaciones informáticas y servicios informáticos.

CAPÍTULO II

PROGRAMAS Y APLICACIONES INFORMÁTICAS DE CÓDIGO ABIERTO

Artículo 23. El Estado promueve la utilización de programas y aplicaciones informáticas que utilicen plataformas de código abierto y de producción nacional, con el objetivo de priorizar su uso e incrementar la soberanía tecnológica y la seguridad nacional.

Artículo 24. El Ministerio de Comunicaciones es el responsable de elaborar, establecer y controlar el plan para la migración de programas y aplicaciones informáticas propietarios hacia plataformas de código abierto de producción nacional, en coordinación con los órganos y organismos de la Administración Central del Estado y el Banco Central de Cuba, así como de adoptar las medidas que garanticen brindar servicios de asesoría técnica, formación del personal y acceso a las aplicaciones de código abierto.

Artículo 25. La migración de programas y aplicaciones informáticas propietarios hacia plataformas de código abierto y de producción nacional se aplica a los órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba; esta migración se realiza de forma ordenada y progresiva, y donde sea imprescindible coexiste con los sistemas propietarios, siempre que satisfagan los requerimientos de seguridad y las necesidades de informatización de cada entidad.

TÍTULO III

GOBIERNO Y COMERCIO ELECTRÓNICO

CAPÍTULO I

GOBIERNO ELECTRÓNICO

Artículo 26. El Estado incorpora el Gobierno Electrónico en la prestación de sus servicios y trámites, la difusión de información e interacción con la población.

Artículo 27. El Gobierno Electrónico es el uso de las TIC en la gestión de la administración pública para incrementar su eficacia y eficiencia, con la finalidad de mejorar la información y los servicios ofrecidos a los ciudadanos, incrementar la transparencia del sector público y la participación de la población.

Artículo 28. El Ministerio de Comunicaciones, en coordinación con otros órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba, elabora las propuestas de acciones para implementar el Gobierno Electrónico.

Artículo 29. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular aplican las acciones aprobadas para establecer el Gobierno Electrónico, con el objetivo de garantizar el máximo aprovechamiento de las TIC y la prestación de servicios eficientes a la población.

Artículo 30. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que tengan a su cargo Registros Públicos, son responsables de su informatización y de priorizar su ejecución.

Artículo 31. Los documentos en formato digital firmados electrónicamente con el empleo de certificados digitales de la Infraestructura Nacional de Llave Pública, conforme a las regulaciones establecidas por la Ley, prueban la autenticidad de la elaboración de estos y son reconocidos como válidos, con plena eficacia por las autoridades y funcionarios públicos a todos los efectos procedentes.

Artículo 32. El Ministro de Justicia, en el marco de su competencia, con la colaboración de los ministerios del Interior y de Comunicaciones y demás órganos y organismos de la Administración Central del Estado, que correspondan, propone, o emite en su caso, las disposiciones jurídicas que resulten necesarias para dotar de validez legal los documentos en formato digital.

Artículo 33. Los datos de carácter personal en soporte electrónico solo se pueden revelar a terceros que posean interés legítimo debidamente acreditado ante autoridad competente o que estén autorizados por el titular de estos datos; ante el incumplimiento de lo dispuesto, se procede conforme a lo establecido en la legislación vigente.

Artículo 34. El jefe de la Oficina Nacional de Estadísticas e Información, en coordinación con el Ministerio de Comunicaciones, establece los procedimientos, normativas y estándares tecnológicos que garanticen la interoperabilidad de la información a nivel nacional y la comparabilidad en el ámbito internacional.

Artículo 35. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular determinan los servicios que brindan a la población, facilitan y optimizan los trámites y el acceso a la información, así como la atención ciudadana en línea, y son responsables del uso de las plataformas tecnológicas que protejan los datos del usuario y garanticen la veracidad y autenticidad de la información.

Artículo 36. Los ministerios de Educación y Educación Superior incluyen temáticas de Gobierno Electrónico en los planes de estudio en todos los niveles de enseñanza, según corresponda.

Artículo 37. Las entidades aportan, en el ejercicio de sus funciones, los recursos materiales y humanos, así como la capacitación necesaria para el desarrollo y uso de las TIC.

CAPÍTULO II
COMERCIO ELECTRÓNICO

Artículo 38. El Comercio Electrónico es la actividad comercial que se desarrolla mediante la utilización de las TIC que comprende promoción, negociación de precios y condiciones de contratación, facturación y pago, entrega de bienes o servicios, así como servicios de posventa, entre otros.

Artículo 39. Corresponde al Ministerio del Comercio Interior, con la participación de los de Comercio Exterior y la Inversión Extranjera, y de Comunicaciones, en coordinación con los organismos mencionados en los artículos 43 y 44, desarrollar las acciones para implementar el Comercio Electrónico, así como la exportación e importación de bienes y servicios vinculados a este.

Artículo 40. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y el sistema empresarial, de acuerdo con sus funciones, crean las condiciones para el desarrollo y la participación en el Comercio Electrónico y realizan actividades de capacitación a los directivos, técnicos y especialistas en esta esfera.

Artículo 41. Las personas naturales y jurídicas que participen en actividades de Comercio Electrónico han de cumplir con la legislación vigente en materia de comercio.

Artículo 42. Las personas naturales y jurídicas que provean bienes y servicios por medios digitales están obligadas a desarrollar un entorno técnicamente seguro para las transacciones comerciales en las que operan, de acuerdo con la legislación vigente.

Artículo 43. Corresponde a los órganos y organismos de la Administración Central del Estado implementar, en el marco de su competencia, las acciones y medidas siguientes:

a) El Ministerio de Comunicaciones garantiza que los proveedores de servicios brinden la conectividad necesaria con la debida seguridad, para desarrollar el Comercio Electrónico en el país;
b) el Ministerio de Economía y Planificación prioriza, según las condiciones existentes, los recursos a destinar por el sistema empresarial para la seguridad, supervisión y desarrollo del Comercio Electrónico;
c) el Ministerio de Justicia, con la participación de los del Comercio Exterior y la Inversión Extranjera, y del Comercio Interior, aprueba las disposiciones jurídicas que resulten necesarias para el intercambio de los documentos en formato digital, relacionados con el Comercio Electrónico;
d) El Ministerio del Transporte realiza los estudios y establece las normas para garantizar los servicios de transportación asociados al Comercio Electrónico;
e) el Ministerio del Comercio Interior, en el marco de su competencia, establece las disposiciones normativas para garantizar el adecuado desarrollo del Comercio Electrónico y las medidas de seguridad, así como los procedimientos de control necesarios;
f) el Ministerio de Cultura establece las disposiciones que le correspondan acerca de la Protección de los Derechos de Autor sobre obras intelectuales que se comercializan a través del Comercio Electrónico; y
g) los ministerios de Educación y Educación Superior incluyen temáticas de Comercio Electrónico en los planes de estudio en todos los niveles de enseñanza, según corresponda.

Artículo 44. El Banco Central de Cuba evalúa y autoriza los instrumentos de pago y sus proveedores de servicios, las infraestructuras y los mecanismos para el procesamiento de los pagos por vía electrónica.

TÍTULO IV
SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA NACIONAL

CAPÍTULO I
SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 45. El Estado identifica las Infraestructuras Críticas de las TIC y su seguridad y protección para un correcto funcionamiento.

Artículo 46. Las Infraestructuras Críticas de las Tecnologías de la Información y la Comunicación son aquellas que soportan los componentes, procesos y servicios esenciales que garanticen las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.

Artículo 47. El Ministerio de Comunicaciones, en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, establece el Programa para el Fortalecimiento de la Ciberseguridad y coordina la participación en las actividades internacionales requeridas a ese fin e implementa su control y fiscalización.

Artículo 48. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular implementan las acciones que se corresponden con la política y estrategias de seguridad de las TIC aprobadas, que se establecen en el programa para su fortalecimiento; entre estas acciones se tienen en cuenta:

a) Las soluciones y la infraestructura que garanticen la autenticación, seguridad, legitimidad y autenticidad para el proceso de informatización del país;
b) la seguridad de los sistemas tecnológicos que procesan información clasificada o sirven de sustento a las Infraestructuras Críticas de las TIC,
c) la investigación, desarrollo, asimilación tecnológica y soporte de soluciones para la seguridad de las TIC de forma sostenible;
d) el perfeccionamiento del proceso de compatibilización de los servicios, tecnologías e inversiones con los órganos de la defensa;
e) la certificación y supervisión de las soluciones, servicios y la infraestructura tecnológica; y
f) la actividad de gestión, control, fiscalización y actuación ante incidentes de la seguridad de las TIC.

Artículo 49. Las personas naturales, usuarios de las TIC, cumplen, en lo que a ellas corresponde, con el programa vigente de fortalecimiento de la seguridad de las TIC.

CAPÍTULO II

DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN PARA LA SEGURIDAD Y LA DEFENSA NACIONAL

Artículo 50. El Ministerio de Comunicaciones, con la participación de los ministerios de las Fuerzas Armadas Revolucionarias, y del Interior, coordina y establece las acciones que permitan mejorar paulatinamente las condiciones de fiabilidad, estabilidad y el uso seguro de las TIC, para respaldar la seguridad y la defensa nacional, de forma paralela con la informatización de la sociedad.

Artículo 51. Los ministerios de las Fuerzas Armadas Revolucionarias, y del Interior, definen los requerimientos técnicos, organizativos y de seguridad de los servicios de interés para el país, soportados en sus infraestructuras tecnológicas.

Artículo 52. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular organizan sus servicios de las TIC, en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias, y del Interior, para responder a las necesidades que el país requiera en situaciones excepcionales y las vinculadas a la seguridad y la defensa nacional.

TÍTULO V

INVESTIGACIÓN, DESARROLLO, INNOVACIÓN TECNOLÓGICA Y CAPITAL HUMANO

CAPÍTULO I

INVESTIGACIÓN, DESARROLLO E INNOVACIÓN TECNOLÓGICA

Artículo 53. Corresponde al Ministerio de Ciencia, Tecnología y Medio Ambiente, en coordinación con los de Educación Superior y de Comunicaciones, establecer un programa de ciencia, tecnología e innovación de las TIC que aproveche las potencialidades del capital humano, de manera especial en las universidades y centros de investigación.

Artículo 54. Los ministerios de Ciencia, Tecnología y Medio Ambiente, y de Comunicaciones, en coordinación con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos

del Poder Popular, establecen los programas de ciencia, tecnología e innovación y las acciones que promuevan la investigación científica e industrial en esta especialidad, de conformidad con los objetivos del presente Decreto-Ley.

Artículo 55. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular implementan las acciones que se corresponden con el programa vigente de ciencia, tecnología e innovación de las TIC y han de garantizar el acceso a Internet de los profesionales.

Artículo 56. El Ministerio de Industrias, en coordinación con el de Comunicaciones, diseña la estrategia para reducir gradualmente la obsolescencia tecnológica con sus planes de producción y sostenibilidad, a partir de las prioridades de informatización de la sociedad.

CAPÍTULO II
CAPITAL HUMANO

Artículo 57. El Ministerio de Comunicaciones fomenta programas de calificación y adiestramiento, a fin de ampliar y actualizar la especialización en las diferentes ramas de las TIC, con especial énfasis en la ciberseguridad, los programas y aplicaciones informáticas de código abierto, el desarrollo técnico y profesional, así como los programas de apoyo a la educación tecnológica, en coordinación con las instituciones de educación media y superior del país.

Artículo 58. Los ministerios de Educación y Educación Superior en coordinación con el de Comunicaciones, desarrollan acciones que:

a) Impulsen la investigación, desarrollo, innovación y producción en las TIC y contribuyan a implementar la introducción de los resultados obtenidos;
b) implementen modelos educativos en todos los niveles de enseñanza, que generen el capital humano con las capacidades para desarrollar, sostener y utilizar las TIC; y
c) desarrollen los programas de capacitación en las diferentes ramas de las TIC, acorde con su complejidad y evolución tecnológica.

Artículo 59. Los ministerios de Comunicaciones y de Trabajo y Seguridad Social, de acuerdo con sus funciones, desarrollan acciones encaminadas a:

a) Actualizar periódicamente los calificadores y jerarquizar los cargos, a partir de la idoneidad demostrada para los diferentes perfiles y el conocimiento real, con la participación de la organización sindical del nivel correspondiente;
b) perfeccionar el proceso de planificación de la formación, así como la demanda y distribución de la fuerza de trabajo calificada; y
c) desarrollar el teletrabajo, en coordinación con los demás órganos y organismos de la Administración Central del Estado.

TÍTULO VI
REGULACIÓN, CONTROL Y FISCALIZACIÓN DEL PROCESO DE INFORMATIZACIÓN EN LA SOCIEDAD CUBANA

CAPÍTULO I
REGULACIÓN, CONTROL Y FISCALIZACIÓN

Artículo 60. El Ministerio de Comunicaciones, con la participación de los del Interior y de las Fuerzas Armadas Revolucionarias, designa las unidades organizativas y entidades que garanticen la regulación, control y fiscalización para asegurar el cumplimiento de lo que establece el presente Decreto-Ley.

Artículo 61. Todo proveedor de servicios públicos de las TIC tiene que brindar al Ministerio de Comunicaciones la información que este determine para el cumplimiento de sus funciones.

Artículo 62. Corresponde a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, las formas asociativas sin fines de lucro, las cooperativas y las organizaciones políticas, sociales y de masas, instrumentar el proceso de informatización en su esfera de actividades e implementar el control y fiscalización que corresponda.

Artículo 63. La Contraloría General de la República, con la participación de los ministerios del Interior, de Finanzas y Precios y de Comunicaciones establece las directrices para el desarrollo de la auditoría a las TIC y la evaluación del Sistema de Control Interno asociado a estas y a la actividad de Comercio Electrónico.

Artículo 64. Las personas naturales y jurídicas, sometidas al control y fiscalización en la esfera de las TIC, colaboran y facilitan la gestión de los funcionarios de las correspondientes entidades o unidades organizativas encargadas de estas funciones, sin perjuicio de los derechos constitucionalmente reconocidos.

Artículo 65. Las autoridades de orden público prestan protección y auxilio a los funcionarios de las correspondientes entidades o unidades organizativas de control y fiscalización en la esfera de las TIC.

CAPÍTULO II
MEDICIÓN DEL PROCESO DE INFORMATIZACIÓN EN LA SOCIEDAD CUBANA

Artículo 66. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular realizan mediciones de los impactos del proceso de informatización, para lo que tienen en cuenta, entre otros, la reducción de gastos, la optimización de la fuerza de trabajo y la calidad del servicio o producto.

Artículo 67. La Oficina Nacional de Estadísticas e Información:

a) Incluye en el Sistema de Información Estadístico Nacional los indicadores, definiciones metodológicas y procedimientos de control de la informatización de la sociedad; y
b) con la colaboración de los ministerios del Comercio Exterior y la Inversión Extranjera, del Comercio Interior y de Economía y Planificación, establece los procedimientos de control estadísticos, los indicadores sobre los bienes y servicios que se comercialicen electrónicamente y sus definiciones metodológicas.

TÍTULO VII
CONTRAVENCIONES Y SANCIONES ASOCIADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LOS RECURSOS ADMINISTRATIVOS PARA SU IMPUGNACIÓN

CAPÍTULO I
DE LAS CONTRAVENCIONES ASOCIADAS A LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 68. Se consideran contravenciones asociadas a las TIC, siempre que no constituyan delitos, las violaciones siguientes:

a) Comercializar programas, aplicaciones y servicios informáticos asociados a estos sin la autorización de los organismos competentes de acuerdo con la legislación vigente;
b) fabricar, comercializar, transferir, instalar equipos y demás dispositivos para brindar, facilitar o recibir servicios asociados a las TIC, sin la correspondiente autorización;

c) diseñar, distribuir o intercambiar códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para su análisis e investigación;
d) adicionar algún equipo de telecomunicaciones/TIC o introducir cualquier tipo de programas y aplicaciones informáticas en una red de datos, ya sea a través de soportes removibles o mediante acceso a redes externas sin la autorización del titular, o no garantizar su compatibilización con las medidas de seguridad establecidas para la protección de la red de datos;
e) acceder sin la autorización o agredir a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente autorizados;
f) hospedar un sitio en servidores ubicados en un país extranjero, que no sea como espejo o réplica del sitio principal en servidores ubicados en territorio nacional;
g) interferir, interceptar, alterar, dañar o destruir datos, información, soportes informáticos, programas o sistemas de información y comunicación de servicios públicos, sociales y administrativos;
h) realizar acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, sin la debida autorización; y
i) difundir, a través de las redes públicas de transmisión de datos, información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas.

CAPÍTULO II
DE LAS SANCIONES

Artículo 69. A la persona natural que contravenga lo dispuesto en los incisos a), e) y f) del Artículo 68 se le impone una multa de mil pesos ($ 1 000 CUP); en caso de ser una persona jurídica, la multa que se le impone es de cinco mil pesos ($ 5 000 CUP).

Artículo 70. A la persona natural que contravenga lo dispuesto en los restantes incisos del Artículo 68 se le impone una multa de tres mil pesos ($ 3 000 CUP); en caso de ser una persona jurídica, la multa que se le impone es de diez mil pesos ($10 000 CUP).

Artículo 71. A los responsables de la comisión de contravenciones establecidas por el presente Decreto-Ley y sus disposiciones complementarias, además de la sanción de multa, se les puede imponer las accesorias siguientes:
a) Decomiso de los equipos y medios utilizados para cometer las contravenciones previstas en el Artículo 68;
b) suspensión de la licencia de forma temporal o la cancelación definitiva; y
c) clausura de las instalaciones.

Artículo 72. La acción administrativa por parte de la autoridad facultada para exigir responsabilidad por las contravenciones reguladas en este Decreto-Ley se aplica inmediatamente a partir de que se detectan y se identifique al comisor.

Artículo 73. Las sanciones previstas en el presente Decreto-Ley se aplican sin perjuicio de la responsabilidad civil, penal, material u otra que pueda ser exigible.

Artículo 74. Los equipos y medios decomisados pasan sin derecho a pago alguno al dominio del Ministerio de Comunicaciones.

Artículo 75. Se faculta al Ministro de Comunicaciones a reglamentar el procedimiento y destino de los equipos y medios decomisados.

Artículo 76. Contra las sanciones previstas en el presente Decreto-Ley se cumple lo establecido en la legislación vigente. No procede la reclamación por los beneficios dejados de percibir a resultas de los daños o perjuicios que pudieran ocasionarse por las medidas aplicadas.

CAPÍTULO III
DE LAS AUTORIDADES FACULTADAS PARA LA IMPOSICIÓN DE SANCIONES

Artículo 77. Los inspectores designados por el Ministerio de Comunicaciones y por las administraciones locales del Poder Popular quedan facultados para imponer la sanción de multa establecida; además de proponer y asistir en la aplicación del decomiso, una vez aprobado por la autoridad facultada designada por el Ministerio de Comunicaciones, a los que infrinjan lo dispuesto en el presente Decreto-Ley y sus disposiciones complementarias.

Artículo 78. Los inspectores designados por el Ministerio de Comunicaciones y por las administraciones locales del Poder Popular quedan facultados para realizar la retención de los objetos sujetos a decomiso, a fin de garantizar su conservación y custodia, previo inventario, e inician el expediente correspondiente; en los casos que así se requiera, son auxiliados en sus actuaciones por la Policía Nacional Revolucionaria.

CAPÍTULO IV
DE LOS RECURSOS Y PLAZOS DE PRESCRIPCIÓN

SECCIÓN PRIMERA
De los Recursos de Apelación y Reforma

Artículo 79. Contra las sanciones de multa impuestas por los inspectores a que se refieren los artículos anteriores, cabe la presentación de Recurso de Apelación ante el jefe de la entidad o unidad organizativa de control y fiscalización del área bajo su jurisdicción y competencia, en el plazo de quince días hábiles, contados a partir de la fecha de su notificación, el que lo resuelve en el plazo de hasta sesenta días hábiles.

Artículo 80. Procede el Recurso de Reforma ante el jefe de la entidad o unidad organizativa de control y fiscalización del área bajo su jurisdicción y competencia en el plazo de quince días hábiles contados a partir de la fecha de su notificación, contra la sanción de decomiso impuesta por la referida autoridad, quien lo resuelve en el plazo de hasta sesenta días hábiles, contados a partir de su interposición.

Artículo 81. El jefe de la entidad o unidad organizativa de control y fiscalización puede declarar inadmisibles los Recursos de Apelación y de Reforma cuando estos se presenten fuera de los términos establecidos. Contra la decisión del jefe de la entidad o unidad organizativa de control y fiscalización procede Recurso de Alzada.

SECCIÓN SEGUNDA
Del Recurso de Alzada

Artículo 82. Contra la resolución que desestime en todo o en parte el Recurso de Apelación o Reforma, según el caso, interpuesto en primera instancia ante el jefe de la entidad o unidad organizativa de control y fiscalización del área bajo su jurisdicción y competencia, procede Recurso de Alzada ante el Ministro de Comunicaciones, en el plazo de quince días hábiles, contados a partir de la notificación de la resolución anterior.

Artículo 83. El Recurso de Alzada es resuelto por el Ministro de Comunicaciones en el plazo de hasta sesenta días hábiles, contados a partir de su interposición; contra esta decisión no cabe recurso alguno por vía administrativa.

Artículo 84. El Ministro de Comunicaciones puede declarar inadmisible el Recurso de Alzada cuando este se presente extemporáneo.

Artículo 85. Contra la resolución que resuelve el Recurso de Alzada, solo procede interponer en un término de treinta días, contados a partir de la notificación de aquella, demanda administrativa en la vía judicial, de acuerdo con el procedimiento establecido en la legislación de procedimiento civil, administrativo, laboral y económico.

Artículo 86. Las resoluciones que resuelven los recursos de Apelación, de Reforma y de Alzada se hacen firmes una vez decursado el término legalmente establecido para impugnarlas en la vía administrativa o judicial, según sea el caso, sin perjuicio del Procedimiento de Revisión que se establece en la presente.

Artículo 87. El Ministro de Comunicaciones excepcionalmente, puede revisar de oficio o por solicitud del reclamante la decisión adoptada y revocarla, antes de que se haya establecido proceso en la vía judicial, siempre que la decisión sea favorable a la persona reclamante.

El Procedimiento de Revisión, expresado en el párrafo anterior, procede cuando existan hechos o pruebas demostrativas que no pudieron ser presentadas en el momento procesal oportuno y que resulten trascendentes al fondo del asunto, o se demuestre que la resolución impugnada infringe la ley por ser improcedente, arbitraria o ilegal.

SECCIÓN TERCERA

De los plazos de prescripción

Artículo 88. La acción administrativa por parte de la autoridad facultada para exigir responsabilidad por las contravenciones reguladas en este Decreto-Ley prescribe transcurrido un año después de su detección y no haber sido identificado el comisor.

Artículo 89. Los plazos para la aplicación de las multas, el decomiso y demás medidas por la autoridad facultada, previstas en los artículos 69, 70 y 71 del presente Decreto-Ley, prescriben al año si no se ejecutan.

El término de prescripción se interrumpe por cualquier acción realizada por la citada autoridad, tendente a hacerla efectiva.

Después de cada interrupción, el término de prescripción comienza a decursar nuevamente.

DISPOSICIONES ESPECIALES

PRIMERA: Se faculta al Ministro de Comunicaciones para dictar, en el ámbito de su competencia, las disposiciones jurídicas que correspondan para la aplicación de lo establecido en el presente Decreto-Ley.

SEGUNDA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas lo establecido en el presente Decreto-Ley, de conformidad con sus estructuras.

DISPOSICIONES FINALES

PRIMERA: El Consejo de Ministros queda encargado de dictar las disposiciones complementarias sobre la Industria de Programas y Aplicaciones Informáticas y sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

SEGUNDA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia dictan las disposiciones legales, realizan el control y la fiscalización y establecen las coordinaciones que resulten necesarias, relativas a la aplicación del presente Decreto-Ley.

TERCERA: El glosario de términos y definiciones anexo al presente Decreto-Ley para su mejor comprensión, forma parte de su contenido.

CUARTA: Derogar las disposiciones siguientes:

1) Acuerdo No. 5586, de 26 de diciembre de 2005, del Consejo de Ministros, que aprueba los Lineamientos para el desarrollo en Cuba del Comercio Electrónico; y

2) Acuerdo No. 6058, de 9 de julio de 2007 del Comité Ejecutivo del Consejo de Ministros, que aprueba los Lineamientos de Seguridad de las tecnologías de la información.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, en La Habana, a los 17 días del mes de diciembre de 2018.

Miguel Díaz-Canel Bermúdez
Presidente del Consejo de Estado

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) **Documento en formato digital:** Es un tipo de contenido que proporciona información o datos, que puede ser procesado, trasmitido o almacenado y tiene la capacidad de proporcionar información de una persona a otra.
2) **Entidad:** Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.
3) **Operador de redes de telecomunicaciones:** Persona jurídica a la que se le otorga una concesión administrativa o autorización, de acuerdo con la legislación vigente, para la instalación, operación, explotación, mantenimiento y comercialización de redes de telecomunicaciones, para ofrecer servicios públicos de telecomunicaciones a usuarios finales.
4) **Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular:** Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado, las organizaciones superiores de dirección empresarial que incluye a la Empresa de Telecomunicaciones de Cuba S.A.
5) **Proveedor de servicios públicos de las TIC:** Persona natural o jurídica, autorizada para prestar servicios de las TIC a terceros.
6) **Servicios de las TIC:** Son aquellos servicios de provisión de hospedaje y alojamiento; de aplicaciones; y de servicios informáticos.

CONSEJO DE MINISTROS

GOC-2019-548-O45

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente de los consejos de Estado y de Ministros de la República de Cuba.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley No. 370 “Sobre la Informatización de la Sociedad en Cuba”, de 17 de diciembre de 2018, en su Disposición Final Primera encarga al Consejo de Ministros dictar disposiciones complementarias sobre la Industria de Programas y Aplicaciones Informáticas.

POR CUANTO: El referido Decreto-Ley No. 370, establece las regulaciones generales aplicables a la determinación del alcance de la Industria Cubana de Programas y Aplicaciones Informáticas para promover, perfeccionar e incrementar la producción nacional y las exportaciones de los productos de la industria y a la sustitución de importaciones, acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o), de la Constitución de la República de Cuba, decreta lo siguiente:

DECRETO No. 359
SOBRE EL DESARROLLO DE LA INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I
OBJETO, OBJETIVOS Y ÁMBITO DE APLICACIÓN

Artículo 1. El Estado promueve el desarrollo y utilización de la Industria Cubana de Programas y Aplicaciones Informáticas, en lo adelante la Industria, con el objetivo de contribuir a respaldar las prioridades de la informatización en beneficio de la economía, la sociedad y la Seguridad y Defensa Nacional, para alcanzar un crecimiento sustancial de su ejecución y servicios asociados.

Artículo 2. El presente Decreto tiene como objeto establecer el marco legal reglamentario que ordene y garantice el derecho al acceso y participación de las personas en el desarrollo de la Industria cubana de programas y aplicaciones informáticas, en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los acuerdos internacionales en esta materia de los que la República de Cuba es Estado parte.

Artículo 3. Resulta de aplicación este Decreto a las relaciones jurídicas que se establecen entre los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, el sistema empresarial y las formas de propiedad y gestión no estatal cuyo objeto social o actividad comprenda el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos asociados a esta industria.

Artículo 4. Los objetivos del presente Decreto son los siguientes:

a) Promover la empresa estatal socialista, como actor principal en esta industria y, de conjunto con las formas de propiedad y gestión no estatal, contribuir a la informatización de la sociedad, la sustitución de importaciones y a las exportaciones;
b) preservar y desarrollar el capital humano asociado a la actividad y estimular su vínculo con las prioridades de informatización de la sociedad;
c) fortalecer la capacidad de la Industria para contribuir a la soberanía tecnológica, la ciberseguridad, la sostenibilidad y crecimiento económico del país y al bienestar social; e
d) impulsar la integración de la investigación, el desarrollo y la innovación con la producción y comercialización de los productos y servicios informáticos.

Artículo 5. La Industria, comprende a las entidades y al trabajador por cuenta propia que se relacionan con el desarrollo de programas y aplicaciones informáticas y la prestación de servicios informáticos, que estén inscritos en el control administrativo del Ministerio de Comunicaciones.

Artículo 6. Las entidades y el trabajador por cuenta propia solicitan al Ministerio de Comunicaciones su incorporación a la Industria, según los requisitos que este establezca.

Artículo 7. Los principios sobre los que se sustenta la Industria cubana de programas y aplicaciones informáticas son:

a) La satisfacción de las exigencias de la informatización de la sociedad cubana;
b) la contribución a la soberanía tecnológica, la ciberseguridad, la sostenibilidad y al crecimiento económico del país;

c) la atención al capital humano asociado a la actividad;
d) la integración de la investigación, el desarrollo y la innovación para la producción y comercialización de productos y servicios;
e) la coherencia en el desarrollo de la Industria y el aprovechamiento de los diferentes actores del modelo económico cubano; y
f) la exportación de productos y servicios, con participación de todas las formas de propiedad y gestión no estatal existentes en el modelo económico cubano.

CAPÍTULO II

ORGANIZACIÓN INSTITUCIONAL Y COMPETENCIAS

Artículo 8. El Ministerio de Comunicaciones es el organismo encargado de proponer, coordinar y controlar el cumplimiento de las políticas y estrategias asociadas al proceso de organización y desarrollo de la Industria y en el ejercicio de sus funciones específicas cumple las acciones siguientes:
a) Propone, coordina, controla y emite directrices asociadas al proceso de organización y desarrollo de la Industria para garantizar el cumplimiento de las normas jurídicas, procedimientos y metodologías y el funcionamiento de los procesos que aseguren su sinergia;
b) inscribe en el control administrativo a las entidades y al trabajador por cuenta propia que conforman la Industria y establece los requisitos que deban cumplir y lo publica en el sitio web;
c) atiende de manera priorizada y diferenciada los proyectos del programa nacional de informatización;
d) promueve y coordina el desarrollo de programas, aplicaciones y servicios informáticos, en correspondencia con las prioridades de informatización del país, así como la capacitación permanente del capital humano de la Industria y el acceso a la información por directivos y funcionarios vinculados a estas actividades, en función de contribuir a la efectividad en el desempeño de su labor;
e) evalúa y controla los planes de acción que desarrollan las entidades y el trabajador por cuenta propia en función del proceso de organización de la Industria, así como asegura el empleo ordenado de las capacidades humanas y tecnológicas del país;
f) diseña e implementa una estrategia de comunicación sobre la Industria y sus resultados, que contribuya al proceso de informatización de la sociedad, así como evalúa sistemáticamente su efectividad;
g) constituye grupos de expertos con el fin de contribuir a la formulación de políticas y estrategias y a la evaluación de su impacto, para proyectar e implementar soluciones informáticas ante los retos que impone el desarrollo y aplicación de las nuevas tecnologías en procesos priorizados de la nación;
h) coordina los esfuerzos nacionales de investigación, desarrollo e innovación en el terreno de las aplicaciones, programas informáticos y servicios asociados; supervisa la protección de sus resultados, en especial los que tengan mayor utilización en los frentes estratégicos del país;
i) impulsa la cooperación internacional y la realización de eventos con la finalidad de lograr una mayor integración de la Industria, ampliar las capacidades del país y asimilar modelos de gestión para el desarrollo de los programas y aplicaciones informáticas y servicios asociados, con el fin de contribuir a la informatización de la sociedad, la prevención y el enfrentamiento a los eventos nocivos en el ciberespacio;

j) aprueba las normas jurídicas asociadas al desarrollo de esta Industria; controla y fiscaliza su cumplimiento; e
k) identifica los principales proyectos informáticos, con el fin de crear las capacidades de desarrollo de la Industria que permitan su impulso.

Artículo 9. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de acuerdo con su misión y funciones específicas aprobadas, desarrollan las acciones que se establecen mediante el presente Decreto, en el marco del proceso de Informatización de la Sociedad Cubana.

CAPÍTULO III
DE LAS ACCIONES PARA FORTALECER LA INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Artículo 10. Corresponde al Ministerio de Comunicaciones, en el marco del proceso de organización y desarrollo de la Industria Cubana de Programas y Aplicaciones Informáticas y de conformidad con sus funciones específicas aprobadas, coordinar con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular competentes, la implementación de las acciones y medidas básicas para de forma integral garantizar el desarrollo de esta Industria.

Artículo 11. En el marco del proceso de organización y desarrollo de la Industria, los organismos de la Administración Central del Estado y el Banco Central de Cuba mencionados a continuación, realizan las acciones y medidas siguientes:

Ministerio del Comercio Exterior y la Inversión Extranjera:

1) Promueve la inversión extranjera y otras formas de asociación, para contribuir al crecimiento de las exportaciones y al progreso de la Industria, en función del interés nacional y la necesidad de potenciar el capital humano;
2) establece e implementa normas que regulen la importación de productos y servicios informáticos en correspondencia con las necesidades del país; e
3) implementa programas de exportación de servicios profesionales especializados en tecnología de la información y la comunicación, en lo adelante TIC e intensifica la cooperación internacional para el intercambio de expertos y la transferencia de tecnologías.

Ministerio de Comunicaciones:

1) Identifica, evalúa y propone políticas y estrategias para la organización de la Industria de programas y aplicaciones informáticas, con el objetivo de fomentar el desarrollo de la empresa estatal informática, de conjunto con las formas de propiedad y gestión no estatal para contribuir al desarrollo de la informatización de la sociedad y a sus exportaciones;
2) adopta un modelo organizativo que garantice el desarrollo y la sostenibilidad económica de la Industria;
3) incrementa la participación de la Industria en los proyectos priorizados por el país y favorece el desarrollo de los programas y aplicaciones informáticas vinculadas a los servicios;
4) favorece la diversificación de entidades especializadas que brinden servicios asociados a las TIC;

5) potencia el desarrollo y alcance de la autoridad nacional de calidad de programas y aplicaciones informáticas y fomenta la creación de empresas estatales que contribuyan de forma intensiva y efectiva a la evaluación, normalización, certificación de la calidad de los programas y aplicaciones informáticas y servicios asociados a las TIC desarrollados en el país, así como promueve la certificación y acreditación de entidades, procesos, especialistas, soluciones y equipamiento informáticos;
6) colabora en la elaboración de los programas de formación y capacitación de especialistas;
7) promueve el desarrollo de parques científicos-tecnológicos como parte integrante de la Industria y para aprovechar la infraestructura y el capital humano de los centros universitarios de nivel superior y potencia la vinculación de la investigación, el desarrollo y la innovación (I+D+i) entre las universidades, los gobiernos locales, los productores de programas y aplicaciones informáticas y los centros de investigación;
8) propone las acciones que favorezcan el fortalecimiento de la empresa estatal informática y su flexibilización en la gestión económica–financiera de estas, permitiéndoles con mayor autonomía, la distribución de utilidades como salario, así como aquellas que contribuyan al incremento de los niveles de exportación de los programas y aplicaciones informáticas y servicios asociados;
9) establece, según lo regulado por el Ministerio del Comercio Exterior y la Inversión Extranjera, el procedimiento para la importación de programas o aplicaciones informáticas;
10) potencia la producción nacional para contribuir a la informatización de la sociedad y a las exigencias en materia de seguridad y soberanía tecnológica;
11) propone formas organizativas para la Industria en correspondencia con las prioridades de informatización de la sociedad y la sustitución de importaciones e implementa la migración ordenada y sostenible a plataformas de código abierto y de producción nacional;
12) prioriza la utilización de código abierto en los proyectos que desarrolle la Industria;
13) atiende el sistema de gestión integrada del capital humano específico para esta Industria que garantice su permanencia en la actividad con el fin de contribuir al mejoramiento de los procesos productivos y de servicios y minimizar el éxodo de personal.
14) atiende a los profesionales del sector informático en función del desarrollo y organización de esta Industria;
15) establece el modelo de calidad para el desarrollo de aplicaciones informáticas (MCDAI);
16) prioriza el desarrollo de las empresas vinculadas de la Industria, así como favorece la aprobación de tarifas preferenciales para los servicios asociados a las redes;
17) regula la participación de las formas de propiedad y de gestión no estatal en el desarrollo de aplicaciones y servicios informáticos;
18) promueve las asociaciones entre entidades para fortalecer la exportación de productos y servicios informáticos;
19) identifica e impulsa la ejecución de proyectos de inversión extranjera y otras formas de relación económica que potencien el mercado nacional, el crecimiento de las exportaciones y el desarrollo del capital humano;

20) fortalece las entidades especializadas de las TIC dirigidas a satisfacer las prioridades de informatización de la sociedad, la seguridad nacional, el desarrollo económico del país, la exportación de productos y servicios y potencia la vinculación de la investigación, el desarrollo y la innovación (I+D+i), así como la generación de empleos y calidad de vida;
21) impulsa la adopción de las normas técnicas internacionales y la emisión de las normas cubanas para las tecnologías, la producción y los servicios informáticos a través del fortalecimiento del trabajo de los comités de normas técnicas;
22) establece el requisito de inscripción de los programas, aplicaciones y servicios informáticos que se desarrollen para su comercialización, en el control administrativo; así como mantiene actualizado el catálogo nacional de soluciones informáticas desarrolladas por la Industria;
23) promueve la seguridad tecnológica en los productos y los servicios informáticos;
24) prioriza el desarrollo de programas y aplicaciones informáticas de producción nacional que sean sistemas operativos, antivirus, herramientas para la planificación de recursos empresariales, plataformas de comercio y gobierno electrónico, programas y aplicaciones informáticas empotradas en equipos tecnológicos producidos en el país, que se establece como única opción de uso en el mercado nacional, excepto aquellos que se autoricen;
25) potencia el desarrollo de aplicaciones y servicios asociados al gobierno y comercio electrónico;
26) promueve la creación de plataformas que faciliten la generación y diversificación de contenidos;
27) promueve el desarrollo de la Industria de equipamiento vinculado a las TIC;
28) inserta la Industria en acuerdos generados por los mecanismos de integración regionales o internacionales para la informatización de las infraestructuras;
29) colabora en el registro y protección de la propiedad intelectual de lo que se genere en este campo para lo que tiene en cuenta las regulaciones vigentes;
30) favorece el empleo de los recursos humanos que componen la Unión de Informáticos de Cuba, como cantera para los proyectos de informatización local, nacional u otros destinados a la exportación; y
31) coordina y participa en la adecuación del marco regulatorio de la industria que contribuya a agilizar su desarrollo y organización.

Ministerios de Ciencia, Tecnología y Medio Ambiente y de Cultura:

1) Proponen o emiten las normas jurídicas relacionadas con la propiedad intelectual y el derecho de autor, respectivamente, en el ámbito del desarrollo, producción y comercialización de programas y aplicaciones informáticas, así como los mecanismos que garanticen la protección del patrimonio nacional del sector.

Ministerio de Economía y Planificación:

1) Dispone, en el marco de su competencia y según el Plan Nacional de Desarrollo Económico y Social, las medidas que favorezcan la sostenibilidad y el fortalecimiento del sistema empresarial estatal y estimulen la producción de programas, aplicaciones y servicios informáticos nacionales; y
2) Establece y controla que en los estudios de factibilidad de las inversiones se tengan en cuenta los presupuestos referidos a programas y aplicaciones informáticas que permitan incrementar las capacidades en la industria nacional, reducir las importaciones, garantizar mayor seguridad nacional y generar productos exportables.

Ministerios de Educación y de Educación Superior, según corresponda:

1) Promueven la vinculación con las entidades de la Industria de los recursos humanos relacionados con la actividad de programas y aplicaciones informáticas de los centros de estudios y de investigación;
2) orientan los programas de las carreras universitarias, de los técnicos superiores y especialidades con perfiles de informática para que permitan la posterior especialización y certificación de competencia en roles profesionales y realizan su revisión periódica para lograr su actualización;
3) tramitan la homologación de cursos de formación o capacitación para que sean certificados en coordinación con entidades y universidades extranjeras;
4) promueven que los egresados de carreras universitarias afines al perfil de informática y los que laboren en las empresas del sector dominen lenguas extranjeras, preferentemente el idioma inglés;
5) garantizan la realización de cursos de formación de postgrado en las TIC para los graduados de otras disciplinas con vistas a elevar el número de expertos;
6) establecen cursos de capacitación para mejorar el desempeño y capacidad del personal de la administración estatal y local en la utilización de productos informáticos de producción nacional para la gestión estatal;
7) desarrollan acciones que impulsen la investigación-desarrollo-producción de programas, aplicaciones y servicios informáticos y contribuye a la introducción de estos resultados;
8) fomentan programas de calificación y adiestramiento, con el objeto de ampliar y actualizar la especialización en las diferentes ramas de la Industria, y enfatizan lo relacionado con la ciberseguridad; a su vez promueven el desarrollo profesional y técnico y los programas de apoyo a la educación tecnológica en la esfera de la informática, en coordinación con las instituciones de educación media y superior del país;
9) implementan programas de capacitación en las diferentes ramas de esta industria, acorde con su desarrollo y evolución tecnológica;
10) mantienen relaciones con las entidades de la Industria que gestionan, producen, desarrollan programas y aplicaciones informáticas y servicios al sector educacional; y
11) desarrollan la preparación permanente del personal asociado a las TIC y a la población en general.

Ministerio de Finanzas y Precios:

1) Implementa mecanismos fiscales que estimulen el desarrollo y la comercialización de la Industria para el mercado nacional y la exportación.

Banco Central de Cuba:

1) Realiza las acciones que se requieran a fin de destinar créditos para el desarrollo de la Industria de programas y aplicaciones informáticas, de acuerdo con lo establecido en materia crediticia.

CAPÍTULO IV
DE LAS OBLIGACIONES, CAPACITACIÓN, INVESTIGACIÓN, DESARROLLO E INNOVACIÓN TECNOLÓGICA

SECCIÓN PRIMERA
De las obligaciones de las entidades y del sistema empresarial vinculadas con la Industria

Artículo 12. Las entidades de la Industria fortalecen sus estructuras y servicios basadas en el uso integrado de las TIC.

Artículo 13. Los dispositivos informáticos son aquellos aparatos tecnológicos que permiten el procesamiento y almacenamiento de la información y la comunicación.

Artículo 14. La Industria y las empresas dedicadas a la producción, importación y comercialización de dispositivos informáticos suscriben acuerdos en interés de favorecer la incorporación de los programas y aplicaciones informáticas desarrolladas en el país.

Artículo 15. Las empresas dedicadas a la producción de dispositivos informáticos en el país garantizan que estos equipos incorporen programas y aplicaciones informáticas de producción nacional.

Artículo 16. Se exceptúan de cumplir lo regulado en el artículo anterior aquellos dispositivos informáticos destinados a la exportación u otros que se autoricen por el Ministro de Comunicaciones.

Artículo 17. Las empresas de la Industria crean capacidades para la prestación de servicios profesionales en materia de consultoría, auditoría, capacitación y entrenamiento.

Artículo 18. Las entidades y el sistema empresarial relacionados con la Industria, implementan las acciones que se corresponden con el programa vigente de investigación, desarrollo e innovación.

SECCIÓN SEGUNDA

De las obligaciones de los ministerios de Ciencia, Tecnología y Medio Ambiente, Comunicaciones, Educación y de Educación Superior

Artículo 19. El Ministerio de Ciencia, Tecnología y Medio Ambiente, en coordinación con los organismos de la Administración Central del Estado y el Banco Central de Cuba, establece el programa de ciencia, tecnología e innovación de la Industria, que aproveche las potencialidades del capital humano, en especial las universidades y centros de investigación.

Artículo 20. Los ministerios de Educación y de Educación Superior:

a) Validan los programas de las carreras en la especialidad de informática, que permitan la especialización y certificación de competencias en roles profesionales, en los niveles medio superior y superior, así como la homologación de los cursos de formación o certificación a cualquier nivel, con entidades y universidades certificadas internacionalmente;
b) combinan la formación, la producción, investigación e innovación y las vinculan con las entidades de la Industria para elevar la calidad de las soluciones informáticas nacionales; y
c) potencian, en coordinación con el Ministerio de Comunicaciones, la capacitación en centros de formación, para lo que tienen en cuenta las normas internacionales, con el objetivo de atraer a personal extranjero a estos centros de formación.

Artículo 21. El Ministerio de Comunicaciones, en coordinación con los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, contribuye a la capacitación del personal en la utilización de programas y aplicaciones informáticas de producción nacional para la gestión de gobierno.

CAPÍTULO V

INDUSTRIA CUBANA DE PROGRAMAS Y APLICACIONES INFORMÁTICAS PARA LA DEFENSA Y SEGURIDAD NACIONAL

Artículo 22. Los ministerios de Comunicaciones, del Interior y de las Fuerzas Armadas Revolucionarias, coordinan y establecen las acciones que permiten alcanzar paulatinamente las condiciones de fiabilidad, estabilidad y seguridad de los programas, aplicaciones y servicios informáticos que respalden la Seguridad y Defensa Nacional.

Artículo 23. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, organizan y establecen los servicios que brinde su Industria, para responder a las necesidades que el país requiera en las diferentes situaciones excepcionales y las vinculadas a la Seguridad y Defensa Nacional.

CAPÍTULO VI

REGULACIÓN, CONTROL Y FISCALIZACIÓN

Artículo 24. El Ministerio de Comunicaciones dispone de las unidades organizativas y entidades que garanticen la regulación, control y fiscalización con el fin de asegurar el cumplimiento de lo que establece el presente Decreto.

Artículo 25. Corresponde a los organismos de la Administración Central del Estado y al Banco Central de Cuba establecer el marco legal que sustente el proceso de ordenamiento en las entidades subordinadas, adscritas, atendidas y patrocinadas relacionadas con la Industria e implementar el control y la fiscalización que corresponda.

Artículo 26. Las personas naturales y jurídicas sometidas a inspección en la esfera de la Industria colaboran y facilitan la gestión de los funcionarios de las correspondientes entidades y unidades organizativas de control y fiscalización sin perjuicio de los derechos legalmente reconocidos.

Artículo 27. Las autoridades de orden público prestan la protección y auxilio a los funcionarios de las entidades y unidades organizativas de control y fiscalización que realizan la inspección en la esfera de la Industria.

DISPOSICIÓN ESPECIAL

ÚNICA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior quedan facultados para adecuar en sus sistemas lo establecido en el presente Decreto.

DISPOSICIÓN TRANSITORIA

ÚNICA: Los órganos, organismos de la Administración Central del Estado y el Banco Central de Cuba ejecutan las medidas necesarias para la migración a la utilización de programas y aplicaciones informáticas de producción nacional antes de que hayan transcurrido tres (3) años, contados a partir de la fecha de entrada en vigor del presente Decreto; y cuando no puedan cumplir con el término establecido, solicitan prórroga al Ministro de Comunicaciones, el que queda facultado para establecer el nuevo término.

DISPOSICIONES FINALES

PRIMERA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización y establecen las coordinaciones que resulten necesarias relativas a la aplicación del presente Decreto.

SEGUNDA: El glosario de términos y definiciones anexo forma parte del contenido del presente Decreto.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 31 días de mes de mayo de 2019.

Miguel Díaz-Canel Bermúdez
Presidente de los consejos
de Estado y de Ministros

Jorge Luis Perdomo Di-Lella
Ministro de Comunicaciones

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) **Entidad:** Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.
2) **Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular:** Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado y las organizaciones superiores de dirección empresarial, que incluye a la Empresa de Telecomunicaciones de Cuba S.A.

GOC-2019-549-O45

MIGUEL DÍAZ-CANEL BERMÚDEZ, Presidente de los consejos de Estado y de Ministros de la República de Cuba.

HAGO SABER: Que el Consejo de Ministros ha considerado lo siguiente:

POR CUANTO: El Decreto-Ley No. 370 “Sobre la Informatización de la Sociedad en Cuba”, de 17 de diciembre de 2018, en su Disposición Final Primera establece que el Consejo de Ministros queda encargado de dictar las disposiciones complementarias sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

POR CUANTO: El referido Decreto-Ley No. 370, dispone las regulaciones generales aplicables a las Tecnologías de la Información y la Comunicación (TIC) y recoge los principios a seguir y las acciones y medidas para la determinación, desarrollo y mejoramiento de las condiciones de fiabilidad, estabilidad y seguridad de las TIC que respalden la informatización de la sociedad y la soberanía de la nación, la investigación, el desarrollo, la asimilación tecnológica y los soportes de soluciones para su seguridad de forma sostenible; acciones que requieren ser implementadas mediante las normas complementarias que resulten necesarias.

POR TANTO: El Consejo de Ministros, en el ejercicio de las atribuciones que le están conferidas en el Artículo 137, incisos ñ) y o) de la Constitución de la República de Cuba, dicta el siguiente:

DECRETO No. 360
SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LA DEFENSA DEL CIBERESPACIO NACIONAL

CAPÍTULO I
OBJETO, OBJETIVOS, DEFINICIONES Y ÁMBITO DE APLICACIÓN

Artículo 1. El Estado moviliza los recursos necesarios para lograr el empleo seguro y eficiente de las Tecnologías de la Información y la Comunicación en función de las necesidades que requiere el desarrollo del país; además, en su papel rector de la sociedad, dirige la implementación de la estrategia aprobada en materia de Seguridad de las Tecnologías de la Información y la Comunicación y controla su cumplimiento, así como promueve la investigación, el desarrollo, la aplicación, la innovación, la divulgación y la capacitación.

Artículo 2. El objeto del presente Decreto es establecer el marco legal que ordene el empleo seguro de las Tecnologías de la Información y la Comunicación, en lo adelante

TIC, para la informatización de la sociedad, la defensa del Ciberespacio Nacional en correspondencia con lo establecido en la Constitución, las leyes y las restantes disposiciones legales relacionadas con el tema, así como los tratados y demás instrumentos jurídicos internacionales de los que la República de Cuba es Estado parte.

Artículo 3. El objetivo general de este Decreto es establecer los niveles de seguridad en correspondencia con los riesgos asociados a la evolución de las TIC y las posibilidades reales de enfrentar estos últimos, y tiene los objetivos específicos siguientes:

a) Proteger el Ciberespacio Nacional y preservar la soberanía sobre su utilización;
b) establecer la seguridad de las TIC y de los servicios y aplicaciones que soportan; así como la de las Infraestructuras Críticas de las TIC con la finalidad de contar con una estrategia de fortalecimiento y sostenibilidad.

Artículo 4. El Ciberespacio es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones, que interactúan entre sí y con las personas, y en el que la información se crea, procesa, almacena y transmite.

Artículo 5. La Ciberseguridad es el estado que se alcanza mediante la aplicación de un sistema de medidas (organizativas, normativas, técnicas, educativas, políticas y diplomáticas), destinado a garantizar la protección y el uso legal del ciberespacio.

En la protección del ciberespacio se incluye la reducción de riesgos y vulnerabilidades, la creación de capacidades para detectar y gestionar eventos e incidentes y el fortalecimiento de la resiliencia.

Artículo 6. La situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema se denomina amenaza.

Artículo 7. Se denomina ataque al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad.

Artículo 8. Se identifica como riesgo a la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático y cause un impacto negativo en la organización.

Artículo 9. La vulnerabilidad se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema.

Artículo 10. El presente Decreto es de aplicación a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, el sistema empresarial y las unidades presupuestadas, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales.

Artículo 11. Constituyen premisas de la seguridad de las TIC para la informatización de la sociedad y la defensa del Ciberespacio Nacional las siguientes:

a) Elevar la Ciberseguridad frente a las amenazas, los ataques y riesgos a los que se exponen las TIC;
b) garantizar que todos los activos de las TIC sean gestionados de acuerdo con los estándares y buenas prácticas en seguridad;

c) aumentar el nivel de atención a la seguridad de las TIC y garantizar que el personal vinculado a estas domine sus deberes y responsabilidades;
d) establecer las bases de un modelo integral de gestión de la seguridad que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales;
e) garantizar el cumplimiento de la legislación vigente en materia de seguridad de las TIC;
f) elevar la seguridad de las TIC mediante el desarrollo de la industria nacional de programas y aplicaciones informáticas;
g) potenciar la preparación de los profesionales de las TIC, la preservación de estos y el desarrollo integral del capital humano asociado a la actividad;
h) concebir la seguridad en todas las etapas de desarrollo e implantación de las TIC;
i) garantizar la seguridad y resiliencia de las redes y los sistemas de información empleados en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular;
j) posibilitar la integración de la investigación, desarrollo e innovación con la producción y comercialización de productos, tecnologías y servicios de seguridad; y
k) promover la cooperación e intercambio internacional en función de la Ciberseguridad y la gobernanza de Internet.

Artículo 12. La Seguridad de las TIC es el conjunto de medidas administrativas, organizativas, físicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC; el empleo del término seguridad informática, tiene igual significado.

CAPÍTULO II
SISTEMA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

SECCIÓN PRIMERA
Estrategia y Planificación

Artículo 13. El Sistema de Seguridad de las TIC es el conjunto de medios humanos, técnicos y administrativos que, de manera interrelacionada garantiza diferentes grados de seguridad informática, en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

Artículo 14. El Sistema de Seguridad de las TIC se constituye a partir de los sistemas de seguridad existentes en las instituciones del país que posean o utilicen las TIC, en interés propio o de terceros, e incluye:
a) Operadores de redes de telecomunicaciones, en lo adelante operadores;
b) proveedores de servicios públicos y privados de acceso a Internet;
c) productor de equipos;
d) proveedor de servicios de red;
e) proveedores de servicios de las TIC;
f) usuarios de las TIC; y
g) entidades encargadas de la dirección, el control y la supervisión de la seguridad de las TIC, así como de las actividades relacionadas con la vigilancia tecnológica, la alerta temprana y la gestión de incidentes.

Artículo 15. Los mecanismos de seguridad comprenden la implementación de hardware o software diseñados o construidos para prevenir, detectar o responder a incidentes de seguridad.

Artículo 16. Se considera un incidente de seguridad cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan.

Artículo 17. Cada entidad que haga uso de las TIC diseña, implanta, gestiona y mantiene actualizado un Sistema de Seguridad, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos.

Artículo 18. A partir del Sistema de Seguridad diseñado, cada entidad elabora su Plan de Seguridad de las TIC.

Artículo 19. El diseño del Sistema de Seguridad de las TIC y la elaboración del Plan de Seguridad de cada entidad se realizan en correspondencia con las metodologías establecidas al respecto por el Ministerio de Comunicaciones.

Artículo 20. El Plan de Seguridad de las TIC de una organización es el documento que incluye, describe y aplica las políticas, medidas y procedimientos diseñados para esta a partir de los riesgos estimados, así como establece las responsabilidades de los diferentes actores que participan en su ejecución.

Artículo 21. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y en aquellas entidades en que la cantidad, diversidad e importancia de las TIC lo requieran, según el análisis que para ello se realice, disponen de los cargos de especialistas de seguridad de las TIC que garanticen la atención de esta actividad.

Artículo 22. Los usuarios de las TIC asumen, en primera instancia, la responsabilidad de las consecuencias que se deriven de su utilización impropia.

SECCIÓN SEGUNDA

Organización institucional, competencias y atribuciones

Artículo 23. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, el sistema empresarial y demás entidades, de acuerdo con su misión y funciones específicas, desarrollan las acciones que se establecen mediante el presente Decreto, en el marco del proceso de Informatización de la Sociedad Cubana.

Artículo 24. El Ministerio de Comunicaciones controla a todos los niveles de dirección de los organismos de la Administración Central del Estado y de las demás personas jurídicas, el cumplimiento de las normas de seguridad de las TIC, excepto aquellos que se determinen por ese propio Ministerio.

Artículo 25. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, establece las normas de seguridad de las TIC y se responsabiliza por la ejecución de las acciones siguientes:

a) Desarrollar y modernizar la infraestructura vinculada a la seguridad de las TIC para incrementar la efectividad en la protección del Ciberespacio Nacional mediante un enfoque sistémico, conceptual y organizativo;
b) impulsar la cooperación internacional y coordinar la participación en eventos que permitan adoptar normas globales para el desarrollo de la Seguridad de las TIC, así como defender la posición del país en materia de Ciberseguridad;
c) suscribir convenios que contribuyan a desarrollar soluciones de seguridad, ampliar el acceso y la transferencia del país a nuevas tecnologías, preparar el capital humano y contribuir al enfrentamiento de las amenazas en el plano internacional;

d) establecer el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad y asegurar los procedimientos para su implementación en todos los niveles por parte de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, así como realizar el enfrentamiento y neutralización de estos sucesos atendiendo a lo que a cada organismo le corresponde;
e) establecer un sistema de trabajo entre las entidades especializadas en seguridad de las TIC que garantice el cumplimiento de sus funciones en el intercambio seguro de información relativa a vulnerabilidades e incidentes de Ciberseguridad, la colaboración y la coordinación entre sí, con el empleo de servicios seguros de voz, videoconferencia y datos;
f) organizar y potenciar de modo sostenible la investigación, el desarrollo, la innovación y el soporte tecnológico, en función de los sistemas para la Seguridad de las TIC;
g) perfeccionar y potenciar la supervisión, certificación, homologación y acreditación de las soluciones, servicios y la infraestructura tecnológica vinculados a la seguridad de las TIC;
h) asimilar y recibir transferencia tecnológica de las infraestructuras técnicas y organizacionales, de hardware y software, en centros de investigación para la seguridad, parques científicos-tecnológicos, los sistemas operativos, los equipos de cómputo y los relacionados con la conectividad;
i) diseñar e implementar acciones de inspección, asistencia, consultoría y auditoría, de la seguridad de las TIC; así como para su control, en correspondencia con la categorización de los sistemas y actividades;
j) ejercer la fiscalización de la seguridad de las TIC;
k) fortalecer la estrategia de desarrollo del antivirus nacional;
l) garantizar el desarrollo de las actividades que los ministerios de las Fuerzas Armadas Revolucionarias y del Interior realizan para la supervisión y el control de los servicios de las TIC;
m) adquirir, asimilar y desarrollar equipamientos y soluciones para la supervisión y control de servicios y aplicaciones con impacto en la Seguridad Nacional;
n) instrumentar los mecanismos que organicen e incentiven la cooperación internacional en función del desarrollo de soluciones y tecnologías de seguridad en el territorio nacional;
o) garantizar el desarrollo de las actividades de supervisión y control de los servicios de las TIC;
p) perfeccionar de forma ordenada los sistemas y mecanismos de supervisión y control existentes sobre las TIC que utilizan el espectro radioeléctrico, así como garantizar la compatibilidad electromagnética y su uso seguro;
q) establecer los requerimientos básicos para las aplicaciones informáticas destinadas a la gestión de incidentes de Ciberseguridad;
r) organizar y controlar la protección de las principales redes informáticas y sistemas de trabajo que generan servicios de esta naturaleza, que constituyen Infraestructuras Críticas de las TIC, para dotarlas del nivel de seguridad en correspondencia con su categoría;
s) certificar la seguridad de las Infraestructuras Críticas de las TIC;
t) establecer e implementar el Sistema Nacional de Certificación de la Seguridad de las TIC y los laboratorios de certificación para evaluarla, en correspondencia con la categorización de los sistemas y actividades;

u) implementar y potenciar la Red de Gobierno con los requerimientos disponibles de máxima seguridad;
v) incrementar y fortalecer mecanismos de seguridad que permitan detectar y prevenir actividades nocivas en las redes informáticas de los operadores, así como en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular y demás entidades;
w) desarrollar e implementar proyectos propios de soluciones integrales, telemática, protección técnica integral y canales colaterales, programas y aplicaciones informáticas básicas, protección de activos digitales, licenciamiento y las soluciones para la Seguridad y Defensa Nacional y el Orden Interior, en correspondencia con la categorización de los sistemas y actividades;
x) desarrollar entrenamientos de Ciberseguridad en los ejercicios que se ejecuten para elevar la defensa del país en el Ciberespacio y comprobar la efectividad de los planes orientados a dar respuesta a incidentes de Seguridad de las TIC; e
y) incrementar la calidad de la gestión del capital humano especializado en la Seguridad de las TIC.

Artículo 26. El Ministerio de Comunicaciones, de conformidad con sus atribuciones y funciones específicas, es el responsable de las actividades siguientes:

a) Fortalecer la infraestructura de seguridad en las redes informáticas;
b) establecer y controlar la implementación de configuraciones básicas de seguridad orientadas al fortalecimiento de las aplicaciones y equipos que operan en el perímetro de las redes informáticas de las entidades;
c) adquirir y desarrollar equipamientos y programas informáticos especializados para el procesamiento y almacenamiento de las evidencias digitales relacionadas con incidentes de Ciberseguridad;
d) facilitar el hospedaje de los servicios de las entidades estatales y del sector no estatal en los centros de datos públicos para garantizar la racionalidad de las infraestructuras de seguridad y su despliegue y minimizar su diseminación;
e) perfeccionar el marco legal con la finalidad de sustentar la seguridad de las TIC en la informatización de la sociedad para establecer interoperabilidad, integridad, confidencialidad, disponibilidad y no repudio de la información;
f) establecer los mecanismos a emplear para la prevención y respuesta a incidentes de seguridad informática que involucren las TIC ubicadas en los hogares y las áreas públicas para el acceso al ciberespacio, por parte de las personas naturales y jurídicas; y
g) garantizar la recopilación de los incidentes de Ciberseguridad que se detecten.

Artículo 27. El Ministerio del Interior, de conjunto con el Ministerio de las Fuerzas Armadas Revolucionarias, de acuerdo con sus funciones específicas, es responsable de fortalecer los mecanismos de seguridad que permitan detectar y prevenir actividades enemigas y delictivas en las redes informáticas de los operadores, así como en las entidades.

Artículo 28. El Ministerio del Interior en coordinación con los ministerios de las Fuerzas Armadas Revolucionarias y de Comunicaciones, realiza las acciones siguientes:

a) Organizar actividades para fortalecer la recopilación y el análisis nacional sobre Seguridad de las TIC; y
b) establecer la gestión de identidad como parte indispensable del proceso de registro y validación, en correspondencia con la legislación vigente.

Artículo 29. El Ministerio de las Fuerzas Armadas Revolucionarias, en coordinación con los ministerios del Interior y de Comunicaciones, mantiene actualizado el Procedimiento para la Compatibilización con la Defensa de los servicios, tecnologías e inversiones vinculadas a las TIC.

SECCIÓN TERCERA

Del empleo seguro de las Tecnologías de la Información y la Comunicación

Artículo 30. La seguridad de la información oficial se rige por la legislación vigente que regula lo relativo a su protección, en cualquier soporte en el que se encuentre.

Artículo 31. Los requerimientos de seguridad para la proyección, diseño e instalación de locales tecnológicos en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, se establecen según lo dispuesto en la legislación vigente.

Artículo 32. Los ministerios del Interior y de Justicia, de acuerdo con sus funciones, son los encargados de regular y controlar la protección de la información correspondiente a las personas naturales y jurídicas y la privacidad de los datos personales.

Artículo 33. La entidad que por sus funciones posea o controle datos de las personas naturales o jurídicas es responsable de la protección de la información personal y la privacidad de los documentos y únicamente facilita a las autoridades competentes la supervisión y acceso a estos datos personales, en correspondencia con la legislación vigente.

Artículo 34. El que haga uso, procese, trasmita y almacene información de personas naturales y jurídicas, lo realiza bajo los principios de legalidad, propiedad y necesidad e indica, de forma explícita, a estas personas los objetivos y el alcance, y han de tener su consentimiento cuando se requiera.

Artículo 35. Las reglas para la recopilación y el uso de la información tienen carácter público y se divulgan de forma oportuna y precisa para garantizar el conocimiento por las personas naturales y jurídicas.

Artículo 36. Se consideran bienes informáticos a los elementos que componen el sistema informático que son protegidos para evitar que sufran algún tipo de daño, como resultado de la materialización de una amenaza.

Artículo 37. Los bienes informáticos de una entidad son utilizados en las funciones propias del trabajo, así como en tareas autorizadas por la dirección de esta.

Artículo 38. Todos los bienes informáticos de una entidad se identifican y controlan, para lo cual se conforma y mantiene actualizado su estado físico, incluidos sus componentes y las especificaciones técnicas de aquellos que pudieran ser sustituidos.

Artículo 39. Es un deber y un derecho de la dirección de la entidad el control y supervisión del correcto empleo de las TIC por parte de los usuarios y su uso no autorizado es sancionable según la legislación vigente.

Artículo 40. Los jefes a cada nivel garantizan que el personal vinculado a las TIC esté capacitado para su utilización, que conozca los deberes y derechos en relación con el Sistema de Seguridad Informática, así como que exista constancia del conocimiento y compromiso que asume este personal de forma individual.

Artículo 41. El Ministerio de Comunicaciones otorga una licencia de operación a las entidades que pueden brindar servicios de seguridad de las TIC a terceros.

Artículo 42. El acceso del personal a las facilidades de procesamiento y a los servicios que brindan las tecnologías requiere de autorización expresa y de un control estricto de su uso por la dirección de cada entidad, las que establecen los requerimientos específicos para garantizar la seguridad, a partir de los riesgos que esto pueda introducir.

Artículo 43. La unidad organizativa que corresponda en cada entidad, de acuerdo con su estructura, exige a los usuarios de las TIC el cumplimiento de la información inmediata de cualquier incidente de seguridad, debilidad o amenaza a los sistemas y servicios con que opera.

Artículo 44. Se denomina Barrera de Protección al dispositivo físico o lógico utilizado para proteger un sistema informático o red de telecomunicaciones y obstaculizar el acceso a estos o entre sus componentes, ya sea de forma directa o remota.

Artículo 45. La dirección de cada entidad determina aquellos equipamientos de las TIC que por las funciones a las que se destinan, la información que contengan y las condiciones de los locales en que se encuentran ubicados, requieren la aplicación específica de medidas especiales de protección física y asegura una barrera de protección a estos medios que impida su empleo en la comisión de hechos intencionales que violen lo establecido o en actividades delictivas.

Artículo 46. El Ministerio de Comunicaciones ejecuta periódicamente las acciones de control a la seguridad de las TIC siguientes:

a) Realizar diagnósticos integrales en los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, tanto tecnológicos como organizativos, que permitan evaluar el estado de la seguridad de las TIC e implementar acciones correctivas para su solución;
b) evaluar sistemáticamente las condiciones de seguridad de las aplicaciones informáticas, tanto en su codificación y despliegue como en la ejecución y trazabilidad de las operaciones realizadas; y
c) diseñar y establecer los mecanismos de comprobación de la Seguridad de las TIC que se utilizan por las personas naturales y jurídicas para acceder al ciberespacio.

Artículo 47. En cada entidad se implementan los controles y procedimientos que los protegen contra programas malignos, con el fin de mitigar sus efectos nocivos e impedir su generalización; para la protección contra virus informático se utilizan los programas antivirus de producción nacional y otros autorizados para su uso en el país, con un soporte establecido que permita su actualización.

Artículo 48. El Virus Informático es el programa capaz de reproducirse a sí mismo sin que el usuario esté consciente de ello; se adiciona a programas de aplicación, así como a componentes ejecutables del sistema, de forma tal que pueda tomar el control de este durante la ejecución del programa infectado.

Artículo 49. Queda prohibido el envío de mensajes masivos que:

a) Sean no deseados (Spam); que se entiende por toda información de voz o datos transmitida o enviada de forma masiva, indiscriminada y repetitivamente por medio de las redes de telecomunicaciones, sin el previo consentimiento de sus destinatarios.
b) no contenga, sea falso u oculto el asunto y la dirección o ubicación física o electrónica, número telefónico, identidad u otro medio de identificación del emisor e impidan a los destinatarios o receptores notificar su voluntad de no recibir más mensajes o no incluyan mecanismos que permitan al receptor manifestar su voluntad de no recibirlos;
c) afecten el uso seguro y la calidad de las redes de telecomunicaciones de Cuba o de otros países o de los servicios que se prestan a través de estas; y
d) posean un contenido que transgreda lo establecido en la legislación vigente cubana o los tratados, convenios o cualquier otro instrumento jurídico de carácter internacional de los que la República de Cuba es Estado parte.

Artículo 50. Los mensajes que contengan las características referidas en el Artículo anterior se consideran mensajes masivos dañinos.

Artículo 51. Corresponde a los operadores y proveedores:

a) Bloquear el envío, recepción o transmisión de los mensajes masivos dañinos que se cursan por sus redes y utilizan sus servicios;
b) suspender temporalmente por hasta un mes las comunicaciones entre sus redes y las que se establecen con las redes de operadores o proveedores extranjeros que no adopten las medidas necesarias para impedir el tráfico de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, dar cuenta al Ministerio de Comunicaciones; y
c) suspender temporalmente por hasta un mes el servicio prestado a los usuarios responsables del envío de mensajes masivos dañinos, lo que se notifica antes de las 72 horas posteriores a su suspensión y, en igual término, da cuenta al Ministerio de Comunicaciones, a los órganos del Ministerio del Interior o de la Fiscalía General de la República.

Artículo 52. En los contratos suscritos por los operadores y proveedores entre sí y con sus usuarios, se incluye una cláusula sobre la responsabilidad derivada del envío de mensajes masivos dañinos a través de las redes de telecomunicaciones con utilización de las TIC o de los equipos terminales de telecomunicaciones que son objeto de control por el Ministerio de Comunicaciones y, ante su incumplimiento, se le aplican las medidas previstas en la legislación vigente.

Artículo 53. Es responsable del envío de mensajes masivos dañinos toda persona natural o jurídica que:

a) directamente los envíe;
b) los genere a través de los equipos de telecomunicaciones de otras personas;
c) los transporte o intermedie en su difusión o trasmisión o haya incidido en su contenido, si mediante sus medios técnicos lo hubiese conocido y no evita su transportación, difusión, trasmisión, envío y reenvío; y
d) cree, venda, preste, intercambie o realice cualquier tipo de recolección o transferencia de listas de direcciones de correo electrónico, números telefónicos u otro medio de identificación del emisor que haya sido realizada sin la autorización o consentimiento de su titular o del operador o proveedor de los servicios y sean conformadas para el envío de mensajes masivos dañinos.

SECCIÓN CUARTA

De la Seguridad de las Operaciones

Artículo 54. La seguridad de las operaciones realizadas sobre las TIC es garantizada por la protección desplegada de seguridad de la red por niveles para evitar interferencias, daños o accesos no autorizados, fugas de datos, robos o falsificación.

Artículo 55. Se denomina traza al registro cronológico de las acciones que se realizan en un sistema, el acceso a este y los procesos y ficheros que han intervenido.

Artículo 56. Los proveedores de servicio de acceso a Internet, para garantizar la seguridad de sus operaciones, cumplen con los deberes siguientes:

a) elaborar procedimientos de operación y gestión de seguridad internos;
b) determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan;
c) adoptar medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;

d) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos;
e) establecer el registro y la trazabilidad de las operaciones realizadas, así como el control de los eventos e incidentes, en correspondencia con las regulaciones vigentes;
f) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles y el cifrado; y
g) establecer la obligatoriedad de las personas naturales y jurídicas de preservar las trazas de los servicios utilizados para acceder al ciberespacio.

Artículo 57. Los responsables de la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad, cumplen con la legislación vigente relativa a los requerimientos de la Seguridad y Defensa Nacional; los requisitos establecidos en las normas nacionales son evaluados por la entidad autorizada por el Ministerio de Comunicaciones a través de la implementación de las medidas siguientes:
a) Establecer un catálogo de equipos y servicios especializados de seguridad considerados como críticos; y
b) promover el reconocimiento recíproco, entre las entidades especializadas en seguridad de las TIC, de certificaciones de seguridad y los resultados de controles, inspecciones y auditorías, para evitar la duplicación de esfuerzos.

Artículo 58. Al determinar las responsabilidades asignadas al personal que labora en las áreas relacionadas con la seguridad informática, se tiene en cuenta el principio de separación de funciones y se especifican las tareas que no pueden ser ejecutadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada, o uso inadecuado de los sistemas de las TIC.

Artículo 59. El jefe de la entidad es el responsable de la introducción de los servicios de las TIC, actualizaciones y nuevas versiones, en correspondencia con el sistema de seguridad establecido y los resultados de las pruebas realizadas, para determinar si cumple los criterios de seguridad apropiados.

Artículo 60. Los sistemas informáticos en que es posible el acceso por múltiples usuarios disponen de un identificador de usuario personal y único; y las personas a las que se le asignen identificadores de usuarios responden por las acciones que con ellos se realicen; en caso del cese de la relación laboral u otras causas que se determine por la dirección de la entidad se procede a eliminar el identificador del usuario; en todos los casos se preservan las trazas de uso de las credenciales de acceso, por un tiempo no menor de un año.

Artículo 61. La entidad establece un procedimiento para la asignación de los identificadores de usuarios en los sistemas, que incluye en el caso de los nuevos la solicitud previa al jefe inmediato superior y su posterior notificación al interesado.

Artículo 62. La entidad implementa un sistema fiable de respaldo de la información esencial para su funcionamiento, que permita su recuperación después de un ataque informático, desastre o fallo de los medios, para ello ejecuta los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

Artículo 63. La información de respaldo, conjuntamente con informes precisos y completos de sus copias y los procedimientos de recuperación documentados, se almacenan en otra ubicación, que le permita no afectarse en caso de desastre en la ubicación principal.

Artículo 64. La información de respaldo requiere una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal; los controles realizados a los medios en la ubicación principal se extienden a los medios de respaldo.

Artículo 65. Los medios de respaldo se prueban regularmente y se verifica el estado de actualización de la información almacenada, con el fin de asegurar la confiabilidad en ellos para un uso de emergencia, cuando sea necesaria la ejecución de un proceso de recuperación.

Artículo 66. El jefe de la entidad establece la utilización obligatoria del antivirus nacional y su despliegue en la red privada.

Artículo 67. El Ministerio de Comunicaciones aprueba la utilización de un antivirus extranjero para su uso en el país, cuando este se justifique, y promueve el fortalecimiento del motor del antivirus nacional a partir de la asimilación de otros motores de antivirus.

Artículo 68. El Ministerio de Comunicaciones promueve el desarrollo y la comercialización de los servicios de instalación y actualización del antivirus nacional y las licencias para su uso por las personas naturales y jurídicas.

Artículo 69. La entidad puede adquirir la infraestructura y el equipamiento especializado necesario para la captura de muestras de programas malignos que incorpora a la base de datos del antivirus nacional.

Artículo 70. El Ministerio de Comunicaciones, en coordinación con los ministerios de Educación y Educación Superior, diseña e implementa proyectos de investigación y desarrollo sobre la seguridad de las TIC en colaboración con centros académicos y de investigación del país, dentro de los que se incluyen los de los ministerios de las Fuerzas Armadas Revolucionarias y del Interior.

SECCIÓN QUINTA

De la seguridad en el empleo de las redes

Artículo 71. Los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, de conjunto con los ministerios de Economía y Planificación y el de Finanzas y Precios, evalúan el respaldo financiero para incrementar la Seguridad de las TIC en las redes informáticas, de manera estable y sostenida, a partir de considerar la importancia de la información y los servicios que sustentan, el que se define en el Plan anual de la Economía.

Artículo 72. En todas las redes de datos se habilitan las opciones de seguridad con que cuentan los sistemas operativos, de forma tal que garanticen la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan la supervisión y auditoría de los principales eventos por un tiempo no menor de un año.

Artículo 73. El jefe del área o de la unidad organizativa que atiende las TIC responde por la implementación y ejecución de los procedimientos y normas que garanticen el empleo seguro de las TIC de forma general y la protección de la seguridad de la red por niveles para evitar interferencias, daños o accesos no autorizados, fugas de datos, robos o falsificación de forma particular; para lograr este objetivo tiene las responsabilidades siguientes:

a) Determinar las personas responsables de la seguridad de la red y los sistemas que soporta, así como implementar mecanismos efectivos de control y supervisión sobre la actividad que realizan, así como aquellos que permitan filtrar o depurar la información que se intercambie.

b) adoptar las medidas técnicas y organizativas para prevenir la contaminación con programas malignos, ataques e intrusiones en la red, así como otras acciones que pongan en peligro la seguridad de las TIC;
c) elaborar planes de respuesta a incidentes de seguridad que establezcan medidas para su prevención y, en caso de ocurrencia, aseguren la actuación bajo el principio de la racionalidad y en correspondencia con lo establecido a esos efectos; y
d) aplicar mecanismos que aseguren la preservación de evidencias digitales, la clasificación de los datos sensibles, el cifrado y las trazas de los servicios utilizados para acceder al ciberespacio por parte de las personas naturales y jurídicas.

Artículo 74. El jefe del área o de la unidad organizativa que atiende las TIC asegura la instalación de las herramientas de seguridad autorizadas por el Ministerio de Comunicaciones para la fiscalización y la supervisión del empleo de las redes de datos y de los servicios implementados.

Artículo 75. La arquitectura y la configuración de los diferentes componentes de seguridad de una red de datos y la implementación de sus servicios están en correspondencia con el Plan de Seguridad de las TIC, y en ningún caso son el resultado de la iniciativa de una persona, con independencia de la preparación que posea.

Artículo 76. Toda red de datos requiere para su operación de la presencia de, al menos, una persona encargada de su administración.

Artículo 77. La gestión de administración de las redes de datos implica la concesión de privilegios requeridos para la tarea que cumple, los que se realizan directamente desde el puesto de trabajo que ocupe; se prohíbe la administración remota de estas redes de datos a través de redes públicas sin mecanismos criptográficos autorizados por los organismos competentes.

Artículo 78. Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las redes son responsables de su propia conducta; para ello conocen y cumplen los planes de seguridad de las TIC.

Artículo 79. Los jefes de las redes de datos o equipos que prevean conexiones desde o hacia el exterior de una entidad, instalan los medios técnicos que aseguren una barrera de protección entre las TIC de la entidad de que se trate y la red externa, con los mecanismos de seguridad que sea necesario implementar.

Artículo 80. La dirección de la entidad instrumenta la ejecución de procedimientos periódicos de verificación de la seguridad de sus redes de datos, con la finalidad de detectar posibles vulnerabilidades, incluido para ello, cuando sea procedente y debido a la sensibilidad de estas acciones, la comprobación de forma remota por entidades autorizadas oficialmente.

Artículo 81. El jefe del área o de la unidad organizativa que atiende las TIC que coloque información en servidores para su acceso público establece las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con sus intereses y los del país.

Artículo 82. Cuando por necesidades de conectividad u otros intereses, la entidad requiere hospedar un sitio en servidores ubicados en un país extranjero, esto se realiza como espejo o réplica del sitio principal en servidores ubicados en Cuba y se establecen las medidas requeridas para garantizar su seguridad, en particular durante el proceso de actualización de la información.

Artículo 83. Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior y los de uso interno deben estar instalados en zonas diferentes de la red, de forma tal que evite la conexión entre estos.

Artículo 84. La dirección de la entidad autoriza el acceso de su personal a Internet y los servicios asociados a este, en correspondencia con sus intereses y necesidades, según las normas particulares establecidas para estos servicios, y documenta esta autorización de manera que pueda ser objeto de comprobación.

Artículo 85. Las redes proveedoras de servicios han de tener las medidas que se requieran para impedir la sobrecarga de los canales de comunicaciones, restringir el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples destinatarios.

Artículo 86. La dirección de la entidad implementa controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

Artículo 87. La dirección de una entidad con redes de datos destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas, cumple los requisitos siguientes:

a) Establecer las medidas y procedimientos de seguridad de las TIC que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que los reciben;
b) implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año;
c) informar a los clientes de estos servicios los requerimientos de seguridad informática que tienen que cumplir, en correspondencia con el Plan de Seguridad de las TIC establecido en la red que los brinda; y
d) facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

Artículo 88. La entidad autorizada es la única que puede explorar o monitorear las redes públicas de transmisión de datos, en busca de vulnerabilidades o información sobre sus usuarios.

Artículo 89. Los productores de equipos, los proveedores de servicios de red y de programas, aplicaciones y servicios informáticos, tanto nacionales como extranjeros, responden por la implementación de los requerimientos que garanticen el empleo seguro de los equipos y servicios que suministran.

Artículo 90. Las personas naturales o jurídicas, nacionales y extranjeras, usuarios de las TIC, responden por la utilización adecuada de los servicios y productos que emplean.

Artículo 91. Los cables de alimentación o de comunicaciones de las redes que transporten datos o apoyen los servicios de información se protegen contra la intercepción o el daño; el tendido de los cables de alimentación eléctrica se realiza de acuerdo con las normas establecidas a esos efectos, separados adecuadamente de los de comunicaciones para evitar posibles interferencias.

Artículo 92. El jefe de cada entidad garantiza que la instalación y operación del equipamiento perimetral de las redes informáticas y los productos especializados de seguridad se realicen en correspondencia con los requerimientos de la seguridad y defensa nacional, y que cumplan los requisitos establecidos en estándares nacionales elaborados a esos efectos y que sean aprobados por una entidad autorizada.

Artículo 93. La entidad aprobada por la autoridad competente para la creación de productos o soluciones informáticas, que implementan herramientas criptográficas, se rige por la legislación vigente.

SECCIÓN SEXTA

Gestión de incidentes de seguridad

Artículo 94. La gestión de incidentes es el proceso que se realiza con el objetivo de prevenir, detectar y enfrentar los de Ciberseguridad y comprende las acciones que se realizan antes, durante y después de su ocurrencia.

Artículo 95. El jefe de la entidad dispone de las medidas y procedimientos que garanticen la continuidad, el restablecimiento y la recuperación de los procesos informáticos, como respuesta a incidentes de Ciberseguridad y en correspondencia con el Modelo de Actuación Nacional.

Artículo 96. Las medidas y procedimientos de recuperación son definidos a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos e incluyen las acciones de respuesta, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

Artículo 97. Los procedimientos para la gestión de incidentes y violaciones de Seguridad de las TIC especifican la obligación de informar su ocurrencia y los pasos a seguir para garantizar una correcta evaluación de lo sucedido, a quién, cómo y cuándo se reporta la respuesta, los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Artículo 98. El Ministerio de Comunicaciones potencia la incorporación del Equipo de Respuesta a Incidentes Computacionales de Cuba a los mecanismos regionales e internacionales que agrupan a ese tipo de organizaciones.

CAPÍTULO III

INFRAESTRUCTURAS CRÍTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 99. El Ministerio de Comunicaciones, en coordinación con los ministerios del Interior y de las Fuerzas Armadas Revolucionarias, es el responsable de elaborar y actualizar el Catálogo Nacional de Infraestructuras Críticas de las TIC y el Plan Nacional para la Protección de las Infraestructuras Críticas de las TIC.

Artículo 100. Los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, según corresponda, establecen y organizan sus Infraestructuras Críticas de las TIC relacionadas con la Seguridad y Defensa Nacional.

Artículo 101. El Ministerio de Comunicaciones, en coordinación con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, organiza el trabajo de protección de las Infraestructuras Críticas de las TIC para dotarlas de la seguridad requerida y controla su correcto despliegue por parte de las entidades especializadas, en correspondencia con el nivel de seguridad requerido.

Artículo 102. El Sistema Nacional de Protección de las Infraestructuras Críticas de las TIC es el conjunto de medidas, previsiones y acciones que se generan, adoptan y ejecutan de forma integral y permanente, con el objetivo de preparar, organizar, ejercer y dirigir la protección de las infraestructuras críticas de las TIC, para lo cual se establecen las políticas, estructuras organizativas, normas y recursos orientados a ese fin, así como se dispone un flujo de información que abarque a todos sus integrantes.

Artículo 103. El Plan Nacional de Protección a las Infraestructuras Críticas de las TIC tiene como objetivo establecer los criterios y las directrices precisas para movilizar las capacidades operativas de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en coordinación con los operadores de las infraestructuras críticas y articular las medidas preventivas necesarias para asegurar su protección permanente, actualizada y homogénea.

Artículo 104. El Ministerio de Comunicaciones, de conjunto con los ministerios de la Fuerzas Armadas Revolucionarias y del Interior, coordina las actividades de prevención, evaluación, aviso, investigación y respuesta a las acciones que afecten el funcionamiento de las Infraestructuras Críticas de las TIC.

Artículo 105. El jefe de la entidad responde por la garantía de la confidencialidad de los datos sobre Infraestructuras Críticas de las TIC a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada; además garantiza que el personal vinculado a las infraestructuras críticas de las TIC esté capacitado para su utilización, posean compromiso político, ético y de responsabilidad social y material; así como que conozcan sus deberes y derechos específicos en relación con estas.

Artículo 106. Los sistemas, las comunicaciones y la información referida a la protección de las Infraestructuras Críticas de las TIC tienen las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

CAPÍTULO IV
DE LA INSPECCIÓN Y LOS INCUMPLIMIENTOS EN LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 107. El Ministerio de Comunicaciones tiene como función estatal la ejecución de las inspecciones en materia de seguridad de las TIC, la que se realiza por sus inspectores y entidades autorizadas por este .

Artículo 108. El jefe de la entidad faculta a especialistas debidamente preparados para realizar controles en materia de seguridad informática a otras entidades atendidas, adscritas, subordinadas y patrocinadas.

Artículo 109. Las entidades y las personas naturales que incumplan lo dispuesto en el presente Decreto y en las disposiciones legales vigentes, están sujetas a la aplicación de las medidas siguientes:

a) Notificación preventiva;
b) invalidación temporal, parcial o cancelación de las autorizaciones administrativas concedidas por el Ministerio de Comunicaciones;
c) suspensión temporal, parcial o la cancelación de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano;
d) decomiso de los medios, instrumentos, equipamientos y otros, utilizados para cometer la infracción; y
e) la aplicación de otras medidas que correspondan, de conformidad con lo legalmente establecido.

Artículo 110. Las entidades y las personas naturales sujetas a la aplicación de las medidas descritas en el Artículo anterior tienen derecho a interponer recurso en la vía administrativa, según lo dispuesto en el Decreto-Ley No. 370, de 17 de diciembre de 2018, “Sobre la Informatización de la Sociedad en Cuba”.

CAPÍTULO V

CAPACITACIÓN Y DIVULGACIÓN SOBRE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 111. El Ministerio de Finanzas y Precios, en coordinación con el Ministerio de Economía y Planificación, define las fuentes de financiamiento, orientadas a la adquisición de tecnologías de seguridad y a la preparación técnica de los especialistas en seguridad de las TIC.

Artículo 112. Los ministerios de Educación y de Educación Superior crean programas educativos y estrategias de trabajo que contribuyan a incrementar la conciencia en la sociedad acerca de la importancia de preservar la información personal.

Artículo 113. El Ministerio de Comunicaciones, en coordinación con el Instituto Cubano de Radio y Televisión, el Ministerio de Cultura y otras instituciones, promueve el uso de los medios de difusión para la trasmisión de mensajes educativos relacionados con la seguridad de las TIC.

Artículo 114. Cada entidad es responsable por la superación de los especialistas en las diferentes áreas del conocimiento, relacionadas con la seguridad de las TIC de acuerdo con su nivel de especialización.

Artículo 115. El jefe de la entidad implementa acciones que contribuyan y propicien la permanencia y el tratamiento diferenciado del personal que cumple funciones como especialistas de seguridad informática, en correspondencia con su categorización.

Artículo 116. La preparación en las materias objeto del presente Decreto de los cuadros, funcionarios y especialistas se desarrolla mediante acciones de carácter educativo-preventivas que estén relacionadas con los planes de estudios de las escuelas o centros docentes que correspondan.

Artículo 117. Los ministerios de Educación y Educación Superior insertan en los planes de estudio los temas referentes a la Seguridad de las TIC en todos los niveles de enseñanza, e implementan planes de estudios para los especialistas en seguridad de las TIC, actualizados por normas internacionales, así como fomentan los intercambios académicos e investigativos con universidades y centros de investigaciones nacionales e internacionales con alta preparación en la temática.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas lo establecido en el presente Decreto, de conformidad con sus estructuras.

DISPOSICIONES FINALES

PRIMERA: Los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización y establecen las coordinaciones que resulten necesarias relativas a la aplicación del presente Decreto.

SEGUNDA: El Ministerio de Trabajo y Seguridad Social actualiza los calificadores y jerarquiza los cargos, a partir de las competencias requeridas para el perfil ocupacional del especialista en seguridad de las TIC.

TERCERA: El glosario de términos y definiciones anexo forma parte del contenido del presente Decreto.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADO en el Palacio de la Revolución, a los 31 días del mes de mayo de 2019.

Miguel Díaz-Canel Bermúdez
Presidente de los consejos
de Estado y de Ministros

Jorge Luis Perdomo Di-Lella
Ministro de Comunicaciones

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1) **Entidad:** Todos los órganos, organismos y entidades nacionales del Estado y del Gobierno, sistema empresarial y unidades presupuestadas, el Banco Central de Cuba y demás instituciones financieras, las cooperativas, las empresas mixtas, las formas asociativas sin ánimos de lucro y las organizaciones políticas, sociales y de masas.
2) **Infraestructuras críticas de las Tecnologías de la Información y la Comunicación:** Son aquellas que soportan los componentes, procesos y servicios esenciales que garantizan las funciones y la seguridad a los sectores estratégicos de la economía, a la Seguridad y Defensa Nacional y a los servicios que brinde la Administración Pública.
3) **Órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular:** Todos los órganos superiores del Estado y del Gobierno, los órganos locales del Poder Popular, los organismos de la Administración Central del Estado, las organizaciones superiores de dirección empresarial que incluye a la Empresa de Telecomunicaciones de Cuba S.A.

____

GOC-2019-550-O45

El Secretario del Consejo de Ministros

CERTIFICA

POR CUANTO: El desarrollo de la infraestructura de conectividad de banda ancha nacional respalda la política a seguir con el fin de lograr mayores capacidades de transmisión de datos y potencialidades para la gestión y control de las redes de telecomunicaciones, que sirva de soporte para la Informatización de la sociedad.

POR CUANTO: Resulta necesario organizar, regular y trazar las líneas para el desarrollo integral de la banda ancha nacional, mediante la aprobación de la Estrategia de Desarrollo de la Banda Ancha en Cuba, que sirva de guía a las entidades nacionales y a la población en el desarrollo, explotación y utilización de los servicios de comunicaciones, así como encargar al Ministro de Comunicaciones con el control de su implementación y de la emisión de las disposiciones normativas complementarias que se requieran para su ejecución ordenada.

POR TANTO: El Consejo de Ministros, en el ejercicio de las facultades otorgadas por el Artículo 137, incisos ñ) y o) de la Constitución de la República de Cuba, y de conformidad con el Decreto-Ley No. 272 “De la Organización y Funcionamiento del Consejo de Ministros”, de 16 de julio de 2010, adoptó el 31 de mayo de 2019 el siguiente:

ACUERDO

PRIMERO: Aprobar la Estrategia de Desarrollo de la Infraestructura de Banda Ancha en Cuba en correspondencia con el Plan Nacional de Desarrollo Económico y Social hasta el 2030, que se anexa al presente y forma parte integrante de este.

SEGUNDO: Encargar al Ministro de Comunicaciones el control de la implementación de lo dispuesto en el apartado Primero y de la emisión de las disposiciones normativas complementarias que se requieran para su ejecución ordenada.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

Y para remitir copia a los miembros del Consejo de Ministros se expide la presente certificación, en el Palacio de la Revolución, a los 31 días del mes de mayo de 2019.

José Amado Ricardo Guerra

ANEXO

ESTRATEGIA DE DESARROLLO DE LA INFRAESTRUCTURA DE BANDA ANCHA EN CUBA

1. Objetivo

Maximizar el impacto de las telecomunicaciones y las tecnologías de la información y la comunicación, en lo adelante TIC, en la transformación y modernización de la economía y la sociedad cubana, así como en la Seguridad y Defensa Nacional, mediante el empleo eficaz e intensivo de las nuevas tecnologías por los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba y demás instituciones financieras, las entidades nacionales, los órganos locales del Poder Popular, el sistema empresarial, las unidades presupuestadas, las formas de propiedad y gestión no estatal, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas, la población en correspondencia con la disponibilidad financiera del país.

2. Alcance

La implementación de la presente estrategia se establece en el marco de una proyección hacia el 2030.

3. Definición de Banda Ancha para Cuba

A los efectos del presente documento, se define como “Banda Ancha” a la tecnología de transmisión de datos que permite descargar contenidos, datos, voz y video de forma simultánea.

4. Modelo de implementación

La prestación de servicios de Banda Ancha requiere de una estructura de red dotada de elementos tecnológicos con mayores capacidades de transmisión y potencialidades para su gestión y control.

La elaboración de un Modelo Tecnológico tiene como objetivo definir la infraestructura que se requiere para la prestación de los servicios propuestos.

Como elemento estratégico debe lograrse una sinergia en el aprovechamiento óptimo de los recursos económicos invertidos por el país en los diferentes sectores, que empleados convenientemente y con alianzas adecuadas para su explotación y comercialización pueden ser estructuras que soporten los servicios de banda ancha, evitándose así inversiones duplicadas.

4.1. Los principales elementos del Modelo Tecnológico son:

a) fortalecer la red de acceso con el empleo de las tecnologías disponibles, en correspondencia con las particularidades de cada territorio o localidad;
b) desarrollar la capa de agregación, en interés de incrementar las capacidades de la red de acceso, especialmente las radiobases de la telefonía móvil; y
c) mejorar y ampliar la capacidad de la red de transporte del dorsal nacional de fibra óptica, en correspondencia con la demanda de ancho de banda que se requiera.

Los órganos, organismos de la Administración Central del Estado, las entidades, los órganos locales del Poder Popular y el Banco Central de Cuba aseguran las acciones necesarias, con el objetivo de alcanzar, de manera acelerada, el uso progresivo de la Banda Ancha y el incremento del acceso de la población a los servicios asociados a la informatización de la sociedad.

4.1.1. Acciones Generales

a) Adecuar el marco regulatorio vigente a los nuevos escenarios y a la introducción de nuevas tecnologías;
b) desarrollar el aprovechamiento óptimo de las fibras ópticas desplegadas y las previstas, así como de otros recursos y facilidades asociadas a las telecomunicaciones y las TIC;
c) fortalecer la capacidad ejecutora del país para facilitar la implementación de la infraestructura de telecomunicaciones en general y en particular de la red para la Banda Ancha;
d) organizar y migrar gradualmente la red al protocolo IPv6, tanto en el acceso como en la capa de transporte;
e) elevar las acciones de formación y capacitación de especialistas en el sector de las Telecomunicaciones y las TIC;
f) introducir gradualmente en el mercado cubano terminales con precios asequibles que soporten los servicios de Banda Ancha;
g) desarrollar la Red Nacional de Educación e Investigación y su conexión con las redes internacionales de educación e investigación.

4.1.2. Acciones específicas. Redes fijas

a) Priorizar el despliegue de las redes provinciales y municipales, que tiene en cuenta, en primer orden, garantizar los anchos de banda requeridos para la conectividad de las radiobases de tecnología 3G y 4G, así como los controladores de acceso de las redes WiFi;
b) comenzar el despliegue de las tecnologías alámbricas en aquellas áreas con redes de cobre flexible;
c) iniciar el despliegue de redes de fibra óptica hasta el lugar (comunidad, edificio, hogar), con el empleo de la tecnología de fibra óptica pasiva (GPON), y priorizar las áreas con mayor densidad poblacional donde no existan otros servicios y aquellas en las que el impacto socioeconómico sea elevado;
d) incorporar en la red nuevas tecnologías flexibles y compactas, que faciliten su rápido despliegue y menores costos, que eviten además las construcciones civiles de alta complejidad;
e) comenzar la migración paulatina de los actuales servicios conmutados de baja velocidad hacia servicios de banda ancha;
f) continuar el despliegue de gabinetes inteligentes y redes de cobre flexibles, y mantener como política que los gabinetes que se adquieran garanticen servicios de telefonía fija y de datos, así como priorizar este en las áreas con mayor densidad poblacional donde no exista ningún tipo de servicio;
g) comenzar el despliegue de la tecnología por cables de cobre (xDSL) en aquellas áreas donde existan las condiciones técnicas;
h) comenzar el despliegue de redes de fibra óptica hasta el usuario (FTTx) principalmente en aquellas áreas en las que el impacto socioeconómico sea elevado;
i) incorporar en los requerimientos constructivos del Instituto de Planificación Física para el diseño de edificaciones y comunidades, los elementos técnicos para el despliegue de redes de fibra óptica y otras facilidades de telecomunicaciones;
j) realizar el despliegue de soluciones combinadas de tecnologías de fibra óptica y cobre.

4.1.3. Acciones específicas. Redes inalámbricas

a) Realizar el despliegue de radiobases de banda ancha móvil en la capital del país y las provinciales, que prioricen aquellas en las que exista conectividad por fibra óptica;

b) impulsar el despliegue de redes WiFi con prioridad en la capital del país, en las provinciales, en las zonas turísticas y en las áreas de alta densidad de usuarios;
c) evaluar el empleo de otras tecnologías que brinden conectividad en las comunidades, con prioridad para estos enlaces dirigido al sector de la educación y la salud;
d) desplegar la tecnología 4G en zonas de alta demanda de tráfico de datos;
e) incrementar el servicio de acceso a Internet sobre tecnología 3G para usuarios nacionales;
f) coubicar radiobases de tecnología móvil en los sitios de la red troncalizada ferroviaria, con el objetivo de aprovechar la infraestructura existente en estos sitios y garantizar este servicio a las localidades aledañas a la red ferroviaria;
g) adquirir tecnologías que aseguren su migración hacia los estándares de 4G y superior;
h) instalar radiobases de nueva generación en las zonas de alto tráfico de voz y datos, y reinstalar las que se sustituyan, para garantizar la voz y datos en aquellos lugares de insuficiente cobertura;
i) preparar la migración de la red de interconexión de las radiobases a la tecnología IP y dejar la tecnología actual como redundancia de estas con el Nodo Central del Sistema;
j) implementar soluciones con celdas pequeñas para mejorar la cobertura de la red móvil, tanto en interiores como en áreas exteriores donde no haya cobertura o exista congestión de las macro celdas, lo que permite aliviar el tráfico de la red celular.

4.1.4. Acciones específicas. Empleo del espectro radioeléctrico

a) Emplear la banda de 1800 MHz (3 canales de 20 MHz) para el despliegue de las tecnologías de 3G y 4G, fundamentalmente para zonas urbanas de alta densidad poblacional;
b) reservar segmento en la banda de 1800 MHz para el despliegue de las tecnologías de 3G y 4G, en interés de usuarios itinerantes que emplean las bandas de Servicios Inalámbricos Avanzados;
c) reservar (en el proceso del “apagón de la TV analógica”) la banda de 700 MHz para el despliegue de tecnologías de 3G y 4G, con el objetivo de asegurar la conectividad en las zonas urbanas de baja densidad poblacional y comunidades;
d) evaluar la reutilización de los segmentos de banda asignados a la difusión de la TV, con el objetivo de brindar conectividad en las comunidades.

4.1.5. Acciones específicas. Desarrollo de las redes de agregación, borde y el dorsal nacional

a) Actualizar y ampliar las capacidades de la Red Dorsal Principal en correspondencia con la demanda;
b) efectuar el despliegue de redes territoriales (provinciales y municipales) en base a redes ópticas de mayor ancho de banda y flexibilidad de conexión;
c) mantener actualizados los protocolos técnicos que permiten el encaminamiento de la transmisión en paquete;
d) fortalecer gradualmente, según la demanda, la Red de Transmisión Internacional avanzando en la migración total a la tecnología IP;
e) asegurar en la arquitectura de la red de telecomunicaciones, los niveles de redundancia requeridos en la Dorsal Principal y en los restantes elementos de red que lo justifiquen (centros de datos, plataformas de control, etc.), para la disminución de vulnerabilidades;
f) incrementar la seguridad de las soluciones de fibras ópticas pasivas mediante configuraciones de anillo.

4.1.6. Acciones específicas. Desarrollo de la capa de gestión, control y supervisión

a) Considerar, en el proceso de migración del control de la red hacia el subsistema de servicios multimedia, los elementos tecnológicos necesarios para el incremento de los servicios de Banda Ancha;
b) adquirir los medios necesarios (equipos y programas de aplicación) para la medición y control de la calidad de los servicios que se prestan;
c) mantener actualizados los planes de señalización, asignación de direcciones IP, sincronización, asignación de bandas de frecuencias y transmisión;
d) actualizar periódicamente el sistema de gestión de todas las capas de red que componen la infraestructura de Banda Ancha.

5. Metas y objetivos específicos para el desarrollo de la Banda Ancha en Cuba

Las metas y objetivos específicos a alcanzar por etapas en el desarrollo de la Banda Ancha se aprueben por el Consejo de Ministros a propuesta del Ministerio de Comunicaciones, que tiene en cuenta las posibilidades económicas del país.

El Ministerio de Comunicaciones establece los indicadores que permitan evaluar el nivel de cumplimiento de las metas y objetivos, así como las velocidades de conexión mínimas a considerar como banda ancha, de acuerdo con la evolución tecnológica que el país alcance de forma paulatina.

MINISTERIO

______

COMUNICACIONES

GOC-2019-551-O45
RESOLUCIÓN 124

POR CUANTO: El Decreto 359 “Sobre el desarrollo de la Industria de Programas y Aplicaciones Informáticas” de 5 de junio de 2019, en su Disposición Final Primera establece que los jefes de los órganos y organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativos a la aplicación de este Decreto.

POR CUANTO: En el proceso de reordenamiento de la industria nacional del software se requiere garantizar la calidad de los programas y aplicaciones informáticos que se desarrollan y comercializan en el país; para alcanzar estos objetivos, es necesario establecer el Reglamento con las acciones a realizar por las personas que desarrollan y comercializan programas y aplicaciones informáticas, disponer las reglas básicas que normen su producción y la evaluación de la calidad de estos procesos productivos y de sus productos resultantes.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO PARA LA PRODUCCIÓN DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS Y LA EVALUACIÓN DE SU CALIDAD

CAPÍTULO I
OBJETO, DEFINICIONES Y GENERALIDADES

Artículo 1. El objeto del presente Reglamento es establecer:

a) Las reglas básicas para la producción de programas y aplicaciones informáticas;
b) la evaluación del proceso de desarrollo de la producción de programas y aplicaciones informáticas;
c) el proceso para la evaluación de la calidad por un tercero de los programas y aplicaciones informáticas.

Artículo 2. El presente Reglamento no incluye la evaluación a los programas y aplicaciones informáticas que constituyan un software empotrado en el equipamiento.

Artículo 3. Este Reglamento es de aplicación a los desarrolladores de programas y aplicaciones informáticas, en lo adelante el desarrollador, a los comercializadores y a los evaluadores autorizados.

Artículo 4. La evaluación de los productos puede ser solicitada por un cliente, por iniciativa del desarrollador o comercializador, cuando se destine a la exportación o se determine por la Dirección General de Informática del Ministerio de Comunicaciones.

Artículo 5. Se autoriza al Centro Nacional de Calidad del Software, en lo adelante Calisoft, como proveedor de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.

CAPÍTULO II
DE LA EVALUACIÓN DE PROCESO

Artículo 6. Los desarrolladores tienen que implementar las reglas básicas para la producción de programas y aplicaciones informáticas, que se relacionan en el Anexo 1 que forma parte integrante de la presente Resolución, y poseer evidencia de su cumplimiento por cada proyecto que ejecute.

Artículo 7.1. La evaluación del proceso de desarrollo se solicita al evaluador autorizado para la validación de la implementación de las reglas básicas; el desarrollador al solicitar la evaluación del proceso entrega sus datos generales o los de la entidad y la evidencia del cumplimiento de las referidas reglas de los proyectos seleccionados.

2. Los documentos a entregar, el procedimiento de evaluación y los resultados de esta, se publican y actualizan en el sitio Web del evaluador autorizado.

Artículo 8. El evaluador autorizado no puede divulgar la información entregada para la evaluación de proceso, ni los datos generados de estas, y garantizan su confidencialidad.

Artículo 9. Los desarrolladores que están certificados con normas nacionales o internacionales para validar la implementación de las reglas básicas para la producción de programas y aplicaciones informáticas, entregan evidencia de la certificación a la Dirección General de Informática y esta evalúa si la norma por la que está certificado, cumple con las reglas básicas; la Dirección General de Informática publica el desarrollador que cumple los requisitos en el sitio Web del Ministerio de Comunicaciones.

CAPÍTULO III
DE LA EVALUACIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Artículo 10. La evaluación de las características de la calidad de programas y aplicaciones informáticas incluye pruebas de usabilidad, adecuación funcional, eficiencia de desempeño, fiabilidad, portabilidad y de seguridad, esta última de acuerdo con la protección de la información y los datos que contiene, evita que otros productos o sistemas tengan capacidad de acceso a los datos según sus tipos y niveles de autorización; la prueba antes mencionada no exime de la realización de la otra evaluación de seguridad establecida por la legislación vigente; el evaluador autorizado publica en su sitio Web las reglas y métricas de las pruebas.

Artículo 11. Al desarrollador y comercializador, que por su naturaleza, destino u otra razón fundamentada sobre su programa y aplicación informática, se le solicita la evaluación de la calidad por la Dirección General de Informática, está obligado a someterlos a la evaluación de la conformidad del evaluador autorizado, o presentar la documentación realizada por un evaluador internacional reconocido en el país.

Artículo 12. Los desarrolladores y comercializadores de productos nacionales o importados y cualquier persona interesada en adquirir un programa y aplicación informática, al solicitar al evaluador autorizado el dictamen técnico sobre la evaluación de la conformidad del producto desarrollado o comercializado, tienen que entregar lo siguiente:

a) El programa o aplicación desarrollada y el paquete de instalación o en su caso el programa de prueba, conocido como demo;
b) especificación de requisitos o funcionalidades;
c) pautas de diseño gráfico, en caso que se requiera;
d) documento con las consultas de la base de datos, si corresponde;
e) manual de usuario;
f) manual o guía de instalación y configuración, si es instalable por el usuario;
g) especificación del entorno donde se usa;
h) diseños de casos de prueba y juegos de datos, en caso que se requiera;
i) especificación de casos de uso o historias de usuario u otro documento técnico que permita detallar los requisitos, cuando se requiera;
j) documento de arquitectura de programa y aplicación informática, cuando corresponda;
k) arquitectura de información, si se requiere
l) certificación emitida por evaluadores internacionales referentes a los procesos y metodologías empleadas en el desarrollo de programas y aplicaciones informáticas, cuando lo posea ;
m) otros que el evaluador autorizado establezca.

Artículo 13. El solicitante presenta al evaluador autorizado la información establecida en el artículo anterior en formato digital, y acompañado de documento que certifica la autenticidad y veracidad de la información, firmada por el jefe de su entidad, o por el interesado, si es una persona natural; el evaluador autorizado puede establecer las particularidades de la entrega, en dependencia del tipo de producto a evaluar, así como mecanismos de entrega en plataformas y servicios de red mediante procedimiento público y actualizado en su sitio web.

Artículo 14. El evaluador autorizado tiene hasta cinco días hábiles para revisar la información presentada y comunicar al solicitante si se le acepta esta o si debe modificarla o completarla.

Artículo 15. La evaluación de la conformidad de un programa y aplicación informática desarrollado o comercializado, tiene una validez de cinco años; decursado este período el producto requiere ser evaluado nuevamente.

Artículo 16.1. En la solicitud de la evaluación de conformidad que se realice, los desarrolladores o el comercializador de un programa y aplicación informática de desarrollo nacional presentan el resultado de la evaluación del proceso de producción de los desarrolladores.

2. Se exceptúa de la presentación del resultado de la evaluación del proceso de producción de los desarrolladores cuando la solicitud la promueva una persona interesada en adquirirlo.

Artículo 17. El evaluador autorizado no puede divulgar la información entregada para la evaluación de los programas y aplicaciones informáticas, ni los datos generados en estas, y acuerda en el contrato suscrito el tratamiento a los productos evaluados con garantía de su confidencialidad, de forma que no viole el derecho de autor sobre estos, en correspondencia con la legislación vigente en la materia.

Artículo 18. En la entrega de los datos considerados como información oficial clasificada, el cliente del servicio de evaluación cumple la legislación vigente en la materia.

Artículo 19.1. El evaluador autorizado, a partir de la información entregada por el solicitante, para realizar la validación correspondiente, tiene que cumplir lo siguiente:

a) Emitir el dictamen técnico sobre la evaluación de la conformidad del programa y aplicación informática desarrollado o comercializado, en un plazo de hasta sesenta días a partir de la notificación al solicitante de la fecha en que comienza el proceso de pruebas o informarle en caso de que no se puede dictaminar y explicar las razones;
b) inscribir el programa o aplicación desarrollada que haya recibido un dictamen técnico favorable en su base de datos de productos evaluados.

2. Los programas y aplicaciones informáticas notificadas con dictamen desfavorable, pueden ser presentados nuevamente cuando se rectifiquen los señalamientos realizados.

CAPÍTULO IV
SOBRE EL EVALUADOR

Artículo 20. El evaluador autorizado es el encargado de la divulgación y actualización en su sitio web de:

a) La documentación necesaria para el solicitante como parte del procedimiento de evaluación: solicitud del servicio, requisitos del servicio y criterios de evaluación;
b) la información que entregan los solicitantes para la evaluación de los procesos productivos y su procedimiento de evaluación;
c) la información que entregan los solicitantes para cada evaluación de los programas y aplicaciones informáticas y su procedimiento con particularidades;
d) los requisitos de calidad y las reglas y métricas con los que son evaluados los programas y aplicaciones informáticas;
e) la información de su base de datos de programas y aplicaciones informáticas validados favorablemente muestra la información general siguiente:
   I. relación de los programas y aplicaciones Informáticas inscritas, sus denominaciones, descripción y versiones;
   II. fecha de evaluación y características evaluadas al programa y aplicación informática;
   III. datos de los titulares de los programas y aplicaciones informáticas inscritos en su base de datos, así como de sus desarrolladores o comercializadores, según corresponda, que incluyen su sitio Web;
f) la información de su base de datos de evaluación de los procesos productivos validados favorablemente, muestra la información general siguiente:
   I. relación de los desarrolladores que han alcanzado el cumplimiento de las reglas básicas;
   II. fecha de evaluación.

Artículo 21. El evaluador autorizado brinda, previa solicitud, una información acordada con los titulares, más completa y detallada de los programas y aplicaciones informáticas inscritas en su base de datos.

Artículo 22. Los resultados de las evaluaciones realizadas por el evaluador autorizado son informados a la Dirección General de Informática.

SEGUNDO: La Dirección General de Informática es la encargada de divulgar y actualizar en el sitio web del Ministerio de Comunicaciones los evaluadores nacionales autorizados, y de diferenciar si se autoriza para la evaluación de procesos o de productos o para ambos.

TERCERO: La no presentación de los resultados de la evaluación del proceso de desarrollo o de la evidencia del cumplimiento de las reglas básicas establecidas en el Anexo 1 de la presente Resolución, es razón invalidante para la solicitud de la evaluación de programas y aplicaciones informáticas de producción nacional, según el plazo dispuesto en la Disposición Final Segunda.

DISPOSICIÓN ESPECIAL

ÚNICA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior, adecuan y regulan, de conformidad con las estructuras y particularidades de estas, la producción y evaluación de programas y aplicaciones informáticas propias para uso en sus sistemas.

DISPOSICIÓN TRANSITORIA

ÚNICA: Encargar al Director General de Informática del Ministerio de Comunicaciones de proponer al que resuelve, en el término de un año, a partir de la puesta en vigor de la presente Resolución, la aprobación del procedimiento y requisitos para la autorización de proveedores de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.

DISPOSICIONES FINALES

PRIMERA: Los desarrolladores tienen un plazo de hasta un año, a partir de la entrada en vigor de la presente Resolución, para establecer en la producción de programas y aplicaciones informáticas, las reglas básicas, y después de este término solicitar la evaluación del proceso productivo.

SEGUNDA: El evaluador autorizado, a partir del plazo de dos años de la entrada en vigor de la presente Resolución, solicita como información obligatoria, la evaluación de proceso productivo del desarrollador, para poder realizar la evaluación de programas y aplicaciones informáticas.

TERCERA: Los directores de la Dirección General de Informática, la Dirección de Inspección y los jefes de las oficinas territoriales de control, del Ministerio de Comunicaciones, y el evaluador autorizado, quedan encargados de controlar el cumplimiento de lo que por la presente se dispone, según corresponda.

CUARTA: El Director General de Calisoft queda responsabilizado con la aprobación de los procedimientos internos para la implementación de lo dispuesto en la presente Resolución a partir de su entrada en vigor.

QUINTA: El glosario de términos y definiciones del Anexo 2 forma parte del contenido de la presente Resolución.

NOTIFÍQUESE a los directores generales de Informática y Calisoft y a los directores territoriales de control, pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas, a los directores de Regulación e Inspección pertenecientes a este Ministerio.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO 1

REGLAS BÁSICAS PARA LA PRODUCCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

1. EN LA GESTIÓN ORGANIZACIONAL

1.1. Determinar los procesos

Implantar y describir los procesos utilizados para el desarrollo de programas y aplicaciones informáticas.

1.2. Determinar los roles y responsabilidades

Identificar y describir los roles y responsabilidades relacionados con el desarrollo de programas y aplicaciones informáticas.

1.3. Desarrollar propuesta de solución

Para cada proyecto informático en lo adelante proyecto, se desarrolla una propuesta inicial de solución técnica que incluye el plan de resultados y el costo del programa y aplicación informática, y tiene en cuenta que:

1. La solución técnica contiene el alcance, los objetivos, los componentes de software del sistema y la tecnología de desarrollo.
2. En la determinación del costo del programa y aplicación informática se tiene en cuenta el resultado de las estimaciones iniciales de parámetros del proyecto tales como: tiempo, esfuerzo y recursos.
3. En los programas y aplicaciones informáticas que se desarrollen a la medida de un cliente, se le entrega la propuesta de solución conciliada.

1.4. Concebir e iniciar el proyecto

Definir formalmente la creación del proyecto y el equipo de trabajo, además de otorgar la autoridad necesaria al jefe de emplear los recursos con que cuente o con los que la organización ponga a su disposición. Se pactan con el cliente los documentos y partes del desarrollo del programa y aplicación informática final que le son entregadas.

1.5. Capacitar al personal

Definir y ejecutar un plan de capacitación al personal vinculado al desarrollo de aplicaciones informáticas, con el objetivo de asegurar que posea las habilidades y competencias necesarias para la ejecución del rol que desempeña.

1.6. Identificar y socializar el conocimiento

Identificar el conocimiento que se genera y que pueda ser utilizado en el desarrollo de aplicaciones informáticas.

El conocimiento identificado se socializa y permite que se encuentre disponible y pueda ser consultado o analizado, según las necesidades específicas.

El conocimiento puede ser tácito o explícito. Tácito se refiere al conocimiento implícito en las personas y explícito se refiere al conocimiento que ha sido documentado y almacenado en algún tipo de medio.

1.7. Proteger los bienes del cliente

Identificar, controlar y salvaguardar los bienes suministrados por el cliente para utilizarlos en el proyecto o incorporarlos al programa y aplicación informática.

2. EN LA GESTIÓN DE PROYECTO

2.1. Definir el alcance y objetivos del proyecto

Especificar el alcance y los objetivos que tiene el proyecto, a partir de las necesidades y restricciones del cliente, así como de la propia organización.

El alcance y los objetivos del proyecto se definen inicialmente como parte de la propuesta de solución técnica a través de la regla 1.3.

2.2. Realizar estimaciones

Especificar la estimación pactada con el cliente con el objetivo de desglosar en actividades la planificación inicial y optimizar los recursos asignados o con los que disponga.

La estimación pactada con el cliente es la estimación inicial de los parámetros del proyecto que se obtiene al cumplir la regla 1.3.

2.3. Definir ciclo de vida del proyecto

Definir el ciclo de vida del proyecto donde se establecen las fases e iteraciones por las que transita. El ciclo de vida es coherente con la metodología seleccionada, el alcance, el entorno, los recursos y las restricciones del proyecto.

2.4. Definir un plan de proyecto

Definir el plan de proyecto que incluya un cronograma de ejecución basado en el ciclo de vida, donde se reflejen los principales hitos y actividades del proyecto. También se planifican todas las áreas de impacto en el cumplimiento de los objetivos, tales como gestión de la calidad, gestión de recursos de riesgos, de requisitos, de la configuración y de adquisiciones, monitoreo y pruebas que se consideren necesarias.

2.5. Monitorear y controlar los planes del proyecto

Monitorear y controlar los planes del proyecto a partir de los valores reales de las tareas y lo planificado inicialmente. Se implementan acciones para resolver y prevenir los problemas cuando ocurran desviaciones de los planes que comprometan el cumplimiento de los hitos del proyecto.

2.6. Identificar necesidades de adquisición

Identificar las necesidades que tiene el proyecto de adquirir productos o componentes de software y analizar sus costos y beneficios.

2.7. Seleccionar proveedores y establecer acuerdo y contrato

Identificar los proveedores potenciales de programa y aplicación informática o componentes de software que cubran las necesidades de adquisición del proyecto y establecer un acuerdo y contrato con los seleccionados.

3. EN LA INGENIERÍA

3.1. Gestionar requisitos

Identificar, especificar e interrelacionar los requisitos del programa y aplicación informática y de sus componentes de software. Los requisitos identificados son aceptados formalmente por el cliente siempre que el desarrollo sea personalizado.

3.2. Desarrollar requisitos

Realizar una descripción técnica de los requisitos y agruparlos acorde con las decisiones arquitectónicas tomadas.

El desarrollo de los requisitos se puede realizar a través de modelos de casos de uso, Modelo del dominio, Escenario de operación, Modelo de proceso de negocio u otros y podrían ser agrupados en módulos o subsistemas.

3.3. Definir la arquitectura del sistema

Definir y aprobar la arquitectura del sistema con los involucrados relevantes, que sirva de base la construcción de la solución y proporcione la información necesaria para su mantenimiento y soporte. La arquitectura contiene:

a. los elementos arquitectónicamente significativos;

b. las definiciones estructurales y la relación entre componentes de software;

c. las principales decisiones arquitectónicas tomadas (patrones, plataforma tecnológica, componentes de software reutilizables);

d. los atributos de calidad a satisfacer con la implementación del programa y aplicación informática.

3.4. Ejecutar pruebas

Ejecutar las pruebas necesarias para verificar los requisitos funcionales y no funcionales del programa y aplicación informática con el apoyo de herramientas manuales o automatizadas que garanticen su objetividad; registrar las no conformidades detectadas y realizar el seguimiento correspondiente.

4. EN EL SOPORTE

4.1. Realizar mediciones a través de indicadores

Establecer indicadores para la gestión del proyecto que permitan satisfacer las necesidades de información a partir de la medición de los objetivos. Analizarlos periódicamente para mantenerlos actualizados.

4.2. Gestionar la Configuración de Software

Identificar los elementos de configuración de software (ECS) y establecer una organización con códigos para cada elemento que permita su mejor identificación y consulta, y disponer un sistema que almacene y controle las versiones. Crear las líneas base y controlar sus cambios, así como las modificaciones de los requisitos de software.

4.3. Realizar el Aseguramiento de la Calidad

Realizar evaluaciones periódicas a la ejecución de los procesos y a sus productos de trabajo, para asegurar la conformidad con los planes, procedimientos y estándares definidos.

Registrar las no conformidades identificadas durante las evaluaciones y asignarle acciones correctivas.

Realizar el seguimiento de las no conformidades hasta la solución definitiva.

ANEXO 2

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1. Componente de software: Elemento de un sistema de software que ofrece un conjunto de servicios, o funcionalidades, a través de interfaces definidas.

2. Evaluador autorizado: Persona jurídica autorizada por el Ministerio de Comunicaciones como proveedor de servicio público de evaluación de procesos y de programas y aplicaciones informáticas.

3. Titular: Persona natural o jurídica propietaria del programa y aplicación informática que es evaluado.

4. Pruebas de usabilidad: Pruebas realizadas a los programas y aplicaciones informáticas para comprobar la factibilidad del uso.

GOC-2019-552-O45

RESOLUCIÓN 125

POR CUANTO: El Decreto 359 “Sobre el desarrollo de la Industria de Programas y Aplicaciones Informáticas” de 5 de junio de 2019 en su Disposición Final Primera establece que los jefes de los órganos y organismos del Estado y del Gobierno y entidades que correspondan, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativos a la aplicación del referido Decreto.

POR CUANTO: La experiencia acumulada en la aplicación de la Resolución 33 del Ministro de la Informática y las Comunicaciones, del 24 de enero de 2008, que establece el Sistema de Inscripción de Productos de Software con el propósito de ordenar los procesos de producción y comercialización en esa industria, aconsejan su actualización para atemperarla a las exigencias del proceso de informatización emprendido en el país, y es necesario emitir una nueva disposición normativa que derogue la referida disposición.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el sistema de inscripción siguiente:

SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

CAPÍTULO I

OBJETIVO, DEFINICIONES Y ALCANCE

Artículo 1. El objetivo del Sistema de Inscripción de los Programas y Aplicaciones Informáticas es ordenar, controlar, almacenar y mantener actualizada la información sobre estos productos existentes en el país.

Artículo 2.1. Son objeto del Sistema de Inscripción de los Programas y Aplicaciones Informáticas, en lo adelante el Sistema, los programas y aplicaciones informáticas de desarrollo y comercialización nacional, destinados a su utilización en el país o a la exportación, así como los de importación; también pueden ser objeto de inscripción a voluntad de sus desarrolladores, aquellos programas y aplicaciones informáticas que no se destinen a la comercialización o que se desarrollen con destinos específicos.

2. Un programa y aplicación informática puede constar de varias versiones (modificaciones específicas) y cada una se inscribe.

Artículo 3. Son sujetos del Sistema las personas naturales y jurídicas, desarrolladoras y comercializadoras de programas y aplicaciones informáticas.

Artículo 4. No son objeto de inscripción los programas y aplicaciones informáticas que constituyan un software empotrado en un equipamiento tecnológico o doméstico.

Artículo 5. Los desarrolladores y comercializadores de programas y aplicaciones informáticas están obligados a inscribirlos a través de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER, previo a su comercialización.

Artículo 6. La inscripción en el Sistema no es constitutiva de derechos de propiedad intelectual sobre dichos programas y aplicaciones informáticas; la realización de este deber no es una exigencia para su posterior inscripción en el Registro de Obras Protegidas y de Actos y Contratos del Derecho de Autor.

CAPÍTULO II

DE LA SOLICITUD DE INSCRIPCIÓN

Artículo 7.1. El desarrollador o comercializador de programas y aplicaciones informáticas a través de la UPTCER, presenta a la Dirección General de Informática del Ministerio de Comunicaciones, la solicitud de inscripción en el Control Administrativo Central Interno, en lo adelante el Control, con la entrega de los modelos A y B que se adjuntan a la presente como anexos 1 y 2, respectivamente, que incluyen las reglas para rellenarlos y que forman parte de la presente.

2. En el caso de la solicitud de inscripción por el comercializador, se presenta adicionalmente:

a) Carta del desarrollador de los programas y aplicaciones informáticas que autoriza al comercializador como representante único para la inscripción;
b) documento oficial que lo acredite para ejercer la actividad de comercialización emitido por el Ministerio correspondiente.

3. Se presenta un modelo B por cada producto que se inscribe y la certificación emitida por la dirección de la persona desarrolladora de programas y aplicaciones informáticas, o por el trabajador por cuenta propia como programador de equipos de cómputo, en el que declare la certeza sobre el funcionamiento y otros atributos del producto, a partir de las pruebas que se le hayan realizado.

4. Además, se entregan los documentos relacionados con los programas y aplicaciones informáticas regulados por las autoridades competentes siguientes:
a) El certificado para programas y aplicaciones informáticas que constituyan Sistemas Contables- Financieros, otorgados a tenor de la legislación vigente del Ministerio de Comunicaciones;
b) el certificado para programas y aplicaciones informáticas médicos, otorgadas al amparo de la legislación vigente sobre la Evaluación Estatal Sanitaria del Ministerio de Salud Pública;
c) la autorización del Ministerio de Justicia para programas y aplicaciones informáticas que gestionen las publicaciones de la Gaceta Oficial de la República.

5. De manera opcional pueden presentarse otros documentos relacionados con la calidad y avales, como el manual de usuario con la especificación de requisitos.

Artículo 8. El Ministerio de Comunicaciones puede solicitar al desarrollador o comercializador otros requisitos adicionales a lo dispuesto en la presente Resolución.

Artículo 9. El Director de la Oficina Territorial de Control, perteneciente al Ministerio de Comunicaciones, donde se detecte que se comercializa un programa y aplicación informática y no está inscrito en el Control, comunica a la autoridad competente, según corresponda, de la infracción cometida y la propuesta de medida a aplicar de acuerdo con su gravedad, para lo que tiene en cuenta las disposiciones legales vigentes en la materia.

Artículo 10. La inscripción de los programas y aplicaciones informáticas tiene una vigencia de cinco años y el productor o comercializador procede a renovarla dentro de los cuarenta y cinco días anteriores a su vencimiento; si no realiza la renovación se cancela de oficio la inscripción, y no puede comercializar el programa y aplicación informática.

Artículo 11. Los desarrolladores y comercializadores de programas y aplicaciones informáticas extranjeras tienen las mismas obligaciones que los desarrolladores y comercializadores nacionales, y cumplen lo dispuesto en la legislación vigente en cuanto a la actividad comercial.

Artículo 12. Por la inscripción del programa y aplicación informática, el desarrollador o comercializador paga cincuenta pesos; el pago se realiza directamente en la sucursal bancaria, según establece la legislación vigente del Ministerio de Finanzas y Precios, y presentan el comprobante de pago a la UPTCER, quien anexa la copia de este al expediente.

Artículo 13. Una vez presentados por el desarrollador o el comercializador los documentos que se establecen en la presente Resolución, y verificada su autenticidad, en un término de quince días, contados a partir de su presentación a la UPTCER, se le otorga la autorización por la Dirección General de Informática y la certificación de inscripción con la numeración correspondiente; este número de inscripción consta en la información de cada producto.

Artículo 14. El programa y aplicación informática puede no aceptarse o cancelarse su inscripción, de no cumplir con la legislación vigente, previa solicitud de la autoridad competente al Ministerio de Comunicaciones y se informa al desarrollador o comercializador.

CAPÍTULO III

DE LA EMISIÓN DE INFORMACIÓN

Artículo 15. La Dirección General de Informática organiza la emisión de la información sobre los programas y aplicaciones informáticas inscritas, a través del sitio web institucional del Ministerio de Comunicaciones, al que pueden acceder las personas interesadas.

Artículo 16. El sitio web institucional del Ministerio de Comunicaciones, contempla sobre los programas y aplicaciones informáticas inscritas la información siguiente:

a) Sus denominaciones y versiones y la fecha de inscripción;
b) información básica sobre el programa y aplicación informática y los certificados y avales que posea;
c) los nombres de los titulares de la inscripción, de los desarrolladores o comercializadores de programas y aplicaciones informáticas y sus datos de contacto.

SEGUNDO: Las funciones establecidas en la presente a la Dirección General de Informática, relativas a la inscripción de programas y aplicaciones informáticas se transfieren por el que suscribe a la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico, una vez esta culmine su proceso de perfeccionamiento funcional, estructural y composicional.

DISPOSICIONES TRANSITORIAS

PRIMERA: Los desarrolladores o comercializadores de programas y aplicaciones informáticas que posean productos que no hayan sido inscritos y que se comercialicen, disponen para inscribirlos en el Control, de un plazo de ciento ochenta días contados a partir de la fecha de entrada en vigor de la presente Resolución.

SEGUNDA: Las inscripciones que se encuentran en trámite a la entrada en vigor de la presente Resolución, continúan este conforme con lo establecido en la legislación por la que lo comenzaron.

DISPOSICIONES FINALES

PRIMERA: El Director General de Informática del Ministerio de Comunicaciones, queda responsabilizado con la elaboración de los procedimientos necesarios internos para la implementación de lo dispuesto en la presente a partir de la fecha de su entrada en vigor.

SEGUNDA: Derogar la Resolución 33 del Ministro de la Informática y las Comunicaciones, de 24 de enero de 2008.

DESE CUENTA a los ministros del Comercio Interior y de Trabajo y Seguridad Social.

NOTIFÍQUESE al director general de informática y al Director de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores territoriales de control, pertenecientes al Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, a los directores generales de Comunicaciones, de la Oficina de Seguridad para las Redes Informáticas y a los directores de Regulación e Inspección, pertenecientes todos al Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO 1

MODELO-A DE DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE LOS PROGRAMAS Y APLICACIONES INFORMÁTICAS

Modelo-A

DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) Denominación de la persona desarrolladora o comercializadora:

____

Código REEUP o No. de Registro o No. de Licencia ________________________

(2) Nombre de la persona :

____

(3) Dirección:

____

____

Teléfono:____________ **FAX**:_____________ **Correo-e**:________________________

(4) Línea del Programa y Aplicación Informática que desarrolla o comercializa:

____

____

(5) Nombre y cargo de la persona de contacto acreditada:

____

Teléfonos:_____________**FAX:**_____________**Correo-e**:________________________

(6) Documento presentado a la Inscripción:

____

____

____

____

Fecha de emisión de la información: ______________________________

_______________________________________ CUÑO

Nombre y firma

REGLAS PARA RELLENAR EL MODELO-A DECLARACIÓN AL SISTEMA DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) - Denominación de la persona desarrolladora o comercializadora del software, así como su código de actividad económica REEUP, número de Registro Mercantil o número de licencia como trabajador por cuenta propia (TPCP) programador de equipos de cómputo.

(2) - Nombre de la persona que ha sido designada al frente de la organización productora o comercializadora del software o nombre del TPCP.

(3) - Dirección completa de la persona desarrolladora o comercializadora (incluir Teléfonos, FAX, correo-e y página Web).

(4) - Línea de los software que desarrolla o comercializa, tales como de gestión económica, educacional, de salud, multimedia, servicios y comercio electrónico y otros.

(5) - Nombre y cargo de la persona autorizada para suministrar la información (incluir Teléfonos, FAX y e-mail para su localización de ser necesario).

(6) - Documentos presentados a la Inscripción: Certificado Comercial expedido por el Registro Central Comercial o Licencia de Trabajador por Cuenta propia de Programador de equipos de cómputo expedido por el MTSS.

ANEXO 2

MODELO-B DE SOLICITUD DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

Modelo-B

SOLICITUD DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) Denominación de la persona desarrolladora o comercializadora:

____

Código REEUP o No. de Registro o No. de Licencia ______________________

(2) Información básica sobre el Programas y Aplicaciones Informáticas

(2.1) Denominación del Programa y Aplicación Informática:

____

____

(2.2) Acrónimo y versión:

____

____

(2.3) País de procedencia del Programa y Aplicación Informática:

____

____

(2.4) Breve descripción del Programa y Aplicación Informática (especificar esfera de aplicación, características, principales funcionalidades y prestaciones)**:**

____

____

____

____

____

____

____

(2.5) Soporte y ayuda al cliente:

____

____

____

Modelo-B reverso

(2.6) Relación de los documentos presentados a la Inscripción:

(Adjuntar otras hojas de ser necesario, se firman cada una de ellas)

____

____

____

____

Fecha de emisión de la información: ____________

____

Nombre y firma

(Para Uso de la Dirección General de Informática)

NÚMERO DE EXPEDIENTE:

REGLAS PARA RELLENAR EL MODELO-B DE INSCRIPCIÓN DE PROGRAMAS Y APLICACIONES INFORMÁTICAS

(1) - Denominación de la persona desarrolladora o comercializadora del software, así como su código de actividad económica REEUP, número de Registro Mercantil o número de licencia para TPCP programador de equipos de cómputo.

(2) - Información básica sobre el Programa y Aplicación Informática.

(2.1) - Denominación del Programa y Aplicación Informática: Denominación (amplia) del producto desarrollado.
(2.2) - Acrónimo y versión: Siglas o identificadores del producto de software, así como la versión del programa y aplicación informática que se comercializa. Por ejemplo: NEON v. 2.5.
(2.3) - País de procedencia del Programa y Aplicación Informática: nombre del país de donde procede el programa y aplicación informática.
(2.4) - Descripción: Breve descripción de los objetivos y prestaciones que brinda el producto desarrollado, indicar esfera de aplicación, plataforma de software y hardware como características de las computadoras, mainframe, estaciones de trabajo, terminales industriales, diferentes tipos de redes sobre los cuales puede trabajar el producto (por ejemplo: Ethernet, UNIX, TCP/IP, Propietaria, Windows, UNIX u otra).
(2.5) - Soporte y ayuda al cliente: En el caso que el producto lo requiera relacionar la documentación desarrollada al efecto y el tipo de ayuda que se le brinda al cliente. (equipo de soporte técnico, visita a los clientes, ayuda en línea).
(2.6) - Relación de los documentos presentados a la Inscripción: Se relaciona toda la documentación que se adjunta a los modelos, tales como: compromiso de certidumbre sobre el funcionamiento y otros atributos del software a partir de las pruebas que se hayan realizado, el Manual de usuario, Manual para la Instalación, u otros y los certificados de cumplimiento de cuestiones legalmente establecidas como son el del MINCOM para software que constituyan Sistemas Contables–Financieros, del MINSAP para software médico y autorización del Ministerio de Justicia para programas y aplicaciones informáticas que gestionen las publicaciones de la Gaceta Oficial de la República.

GOC-2019-553-O45
RESOLUCIÓN 126

POR CUANTO: El Acuerdo 8151, de 22 de mayo de 2017, del Consejo de Ministros, en sus numerales Tercero, Duodécimo y Decimonoveno del Apartado Primero, establece que el Ministerio de Comunicaciones es el organismo encargado de proponer, y una vez aprobada, ejecutar y controlar la política sobre el uso del ciberespacio, así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa; regular y controlar la aplicación de las normas técnicas y operacionales de los sistemas de comunicaciones y las redes informáticas en general que funcionan en el país, encaminadas al desarrollo tecnológico; y autorizar la asignación de los recursos de numeración, de Internet y de uso conjunto a los operadores de servicios público de telecomunicaciones.

POR CUANTO: La Resolución 128 del 24 de junio de 2019, del Ministro de Comunicaciones, que aprobó el Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación establece que en las redes informáticas se tienen que implementar mecanismos de seguridad, que garanticen su protección, por lo que procede disponer de un conjunto de medidas de control, que incluye los tipos de herramientas de seguridad que operan en las redes privadas de datos del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el presente Reglamento que establece las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas de datos, inscritas en el Control Administrativo Central Interno del Ministerio de Comunicaciones.

SEGUNDO: Los titulares o los jefes administrativos de redes privadas de datos son los responsables de la implementación en sus redes de las medidas de control y los tipos de herramientas de seguridad que por la presente se establecen y de que estas sean de código abierto, preferentemente.

TERCERO: La Dirección de Control de acceso al medio, por sus siglas en inglés MAC, es la dirección física, única de cada dispositivo de red y herramienta de seguridad al dispositivo de hardware o software diseñado para proporcionar o comprobar la seguridad en un sistema informático.

CUARTO: Las medidas de control que se establecen son las siguientes:

a) Monitoreo físico e inspección visual al sistema de red, con registros trimestrales;
b) registros actualizados de infraestructura: cableado, enrutadores, conmutadores, terminales, servidores y puntos de acceso, AP de redes inalámbricas;
c) barreras de protección entre las tecnologías de la información y la comunicación que brindan servicios al interior de la red y las redes externas a estas;
d) procedimiento donde se regula el sistema para el uso de las contraseñas de usuarios y dispositivos de la red, la autenticación de usuarios, denominación de equipos y el direccionamiento IP, tiene en cuenta que en las redes inalámbricas no sea dinámico, la deshabilitación de protocolos innecesarios en los enrutadores, la desconexión de los AP sin uso, la activación del filtrado por direcciones MAC, y la encriptación en la configuración de la conexión que lo requiera, así como la legislación vigente sobre este tema;
e) procedimiento donde se definen los tipos de sistemas de supervisión, control, detección y alarma que permiten reaccionar proactivamente y dar una respuesta efectiva ante amenazas de ciberseguridad;
f) procedimiento para que los administradores de redes puedan proponer herramientas complementarias y exista un mecanismo de autorización para incorporarlas;
g) crear un repositorio interno y su sistema de salvas que permita aplicar la gestión de las actualizaciones de seguridad;
h) la gestión de las trazas de los servicios y sistemas informáticos;
i) la implementación de la revisión de los sistemas y servicios que se instalen o empleen.

QUINTO: Las herramientas de seguridad, de las cuales se brinda información sobre sus funciones en el anexo que es parte integrante de la presente Resolución, cumplen los objetivos siguientes:

a) Mostrar el estado actualizado de los servicios implementados en cada servidor;
b) supervisar la carga y disponibilidad de los servidores;
c) establecer un Sistema de Detección y Prevención de Intrusos, por sus siglas en inglés IDS/IPS;
d) monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías;
e) dar seguimiento a las trazas;
f) detectar posibles vulnerabilidades en la red;
g) controlar centralizadamente el estado físico del hardware y del software;
h) gestionar las actualizaciones de seguridad;
i) establecer un sistema de correlación de eventos;
j) realizar el aviso oportuno ante la detección de anomalías o eventos de ciberseguridad.

SEXTO: El empleo de los medios de control y herramientas de seguridad permite:

a) La planificación de su expansión y el perfeccionamiento de la prestación de sus servicios;

b) la detección de fallos e incidentes y su investigación;
c) la ejecución de las pruebas, de acuerdo con lo establecido;
d) el desarrollo de las auditorías informáticas internas o externas, que se ejecuten.

SÉPTIMO: En computadoras o servidores habilitados se instalan barreras y otros medios de protección y se incorporan herramientas de seguridad que permitan el control y monitoreo de los servidores, servicios y usuarios de la red.

OCTAVO: En las computadoras o servidores que constituyen la subred de las terminales de los usuarios de acuerdo al rango IP y nivel de cliente y la subred de los servidores según rango IP y nivel de servidor, se instalan las herramientas que propicien las barreras de protección a los efectos de aplicar políticas convenientes para la aceptación y denegación de tráfico de paquetes.

NOVENO: Las direcciones generales de Defensa, Informática y Comunicaciones, la Dirección de Inspección, la Oficina de Seguridad de las Redes Informáticas y las oficinas territoriales de control, quedan encargadas del control y fiscalización, en lo que a cada cual le corresponda, así como la implementación de las medidas que se requieran para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas.

DESE CUENTA a los jefes de los órganos y organismos de la Administración Central del Estado y de entidades nacionales.

NOTIFÍQUESE a los directores generales de Defensa, Informática, Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas, al director de Inspección y a los directores territoriales de control del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros y al director de Regulaciones del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO

FUNCIONES QUE CUMPLEN LAS HERRAMIENTAS DE SEGURIDAD QUE SE UTILICEN EN LAS REDES INFORMÁTICAS

Las herramientas de seguridad según su tipo cumplen determinadas funciones.

1. Herramientas que muestren el estado actualizado de los servicios implementados en cada servidor

Su función es alertar sobre problemas en la red. La aplicación de la monitorización permite realizar chequeos intermitentes en los equipos (hardware) y en los servicios (software) que se especifiquen con el uso de complementos (plugins en inglés) externos, los que devuelven información al sistema informático. Envía notificaciones de eventos sucedidos de varias maneras (e-mail, mensajería instantánea, SMS). Brinda información del estado actual, histórico del registro oficial de eventos (logs en inglés) e informes que pueden ser consultados vía web.

Se trata de software que proporciona gran versatilidad para consultar cualquier parámetro de interés de un sistema, y genera alertas, que se reciben por medio de correos electrónicos y SMS, entre otros, cuando estos parámetros exceden los márgenes definidos por el administrador de la red.

2. Herramientas para supervisar la carga y disponibilidad de los servidores

Herramientas que permiten la monitorización de redes, vigilan los equipos (hardware) y servicios (software) que se especifiquen, alertan cuando su comportamiento no es el adecuado. Pueden realizar el monitoreo de los servicios de red (SMTP, POP3, HTTP, SNMP), la monitorización de los recursos de sistemas de hardware (carga del procesador, uso de los discos, memoria, estado de los puertos).

Proporcionan una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y generan alertas, que pueden ser recibidas por los responsables a través, entre otros, de correos electrónicos y mensajes SMS, cuando estos parámetros exceden los permitidos por el administrador de la red.

3. Sistemas de Detección y Prevención de Intrusos (IDS/IPS en inglés)

Son capaces de generar análisis del tráfico en tiempo real y registro oficial de eventos (logs en inglés) de paquetes en redes IP. Pueden realizar análisis de protocolos, búsqueda de patrones establecidos y usar para detectar gran variedad de ataques e intentos, tales como almacenamiento y control de desbordamiento de buffer (buffer overflows en inglés), escaneos de puertos silenciosos, ataques interfaz de entrada común (conocidos como Common Gateway Interface (CGI) en inglés) escaneos de tipo protocolo de red en la capa de red del modelo OSI ((conocidos como Server Message Block (SMB) en inglés)), intentos de huellas de Sistemas Operativos (OS fingerprinting) y muchos más. Además, protegen los sistemas computacionales de ataques tanto internos como externos, de manera proactiva; con el uso de tecnologías de detección basada en firmas, en políticas, en anomalías o por medio de sensores. Los sistemas IDS/IPS son usados en conjunto.

4. Herramientas para monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías

Su función es monitorear el comportamiento del tráfico de la red, los más empleados son los graficadores de tráfico multi-enrutadores (MRTG en inglés), que son herramientas para monitorear la progresión del tráfico entrante o saliente de las interfaces del enrutador o el estado de una red, a partir del protocolo simple de Administración de red ((conocido como Simple Network Management Protocol) (SNMP)); existen multitud de herramientas o software que generan páginas HTML (siglas de HipertextMarkupLanguage) (lenguaje de marcado de hipertexto en español) que contienen archivos de imágenes, y proporcionan una información visual en línea del tráfico de los dispositivos.

También son importantes en este tipo de herramientas los Analizadores de protocolos. Existen otros ejemplos de herramientas de seguridad que posibilitan el monitoreo pasivo de una red, y recolectan datos sobre protocolos y hosts. Entre sus características y funcionalidades tiene las de analizar los paquetes que generan tráfico en la red; listar y ordenar el tráfico de red de acuerdo con varios protocolos; identificar pasivamente información relacionada con los hosts de la red, que incluye el sistema operativo ejecutado y direcciones de e-mail del usuario de la estación; mostrar la distribución de tráfico IP entre varios protocolos de la capa de aplicación y decodificar varios protocolos de la capa de aplicación, incluso los encontrados en software de tipo red de pares (Peer to Peer en inglés) (P2).

5. Herramientas para dar seguimiento a las trazas o logs

Estas herramientas realizan análisis de logs (registro oficial de eventos en español) y generan los reportes asociados. Los logs pueden ser los asociados a los servicios web, media, e-mail, registros de seguridad, redes y de aplicaciones. Son herramientas que permiten a los administradores de sistemas informáticos ver de una manera sencilla y amigable qué sitios de Internet se visitan (inclusive se puede saber hasta la hora en que se visitó). Pueden generar listados diarios, semanales, mensuales y personalizados con los sitios de Internet que visita cada usuario, cuánto consumió (MB), y otros. También pueden generar una lista de los sitios más visitados (Top Sites).

6. Herramientas para la detección de posibles vulnerabilidades en la red

Son empleadas para explorar, administrar y auditar la seguridad de redes. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones que corren en ellos, su sistema operativo, así como qué cortafuegos (firewalls/filtros) corren en una red. Realizan un chequeo exhaustivo de potenciales problemas en el servidor, existencia de archivos y aplicaciones peligrosas.

Algunas de estas pueden ser actualizadas vía web y buscan fallas en diferentes categorías, como errores de configuración, archivos por defecto, por ejemplos, archivos y scripts inseguros y versiones desactualizadas de productos; pueden ser utilizadas para hacer trabajos de auditoría de redes y pueden ser diseñadas con el fin de llevar a cabo escaneos rápidos en una gran cantidad de redes, pero es igualmente útil en hosts individuales.

7. Herramientas para el control centralizado del inventario de hardware y del software

Empleadas para el control remoto por los administradores de redes del inventario de hardware y del software. Algunas de ellas permiten también escanear una dirección IP o una subred con el objetivo de obtener información detallada de equipos no inventariados. Pueden adicionalmente, incluir la capacidad de distribución o despliegue de paquetes en las computadoras clientes. Desde el servidor central de gestión, se pueden subir paquetes (configuración de software, comandos o simplemente ficheros a almacenar) que son descargados vía HTTP/HTTPS y son lanzados en el ordenador cliente.

Existen otras que consisten en herramientas de monitorización de seguridad para administradores de redes y agrupan programas libres, como cortafuegos, detectores de intrusos o antivirus, además del repositorio institucional, pueden descargarse gratuitamente de Internet. Su función no es solo poner a trabajar juntos estos programas, sino que se encargan de recoger y ordenar la información que generan y la cruzan, para hacer valoraciones sobre el estado de la red o buscar patrones que sirvan para detectar si es atacada.

8. Gestión de actualizaciones de seguridad

La actualización de las herramientas de seguridad es muy necesaria para eliminar los problemas de seguridad, lo cual permite mantener la eficiencia operativa y la estabilidad en la infraestructura de los sistemas. Debido a la naturaleza cambiante de la tecnología y la aparición continua de nuevas amenazas de seguridad, es necesario tener en cuenta la tarea de la actualización oportuna de las herramientas de seguridad en uso.

En esta tipología se encuentran los repositorios de Software Libre que son una colección de paquetes de programas de una distribución de Linux específica que generalmente contiene archivos binarios precompilados que pueden ser descargados e instalados por los usuarios de su distribución. Es posible también encontrar paquetes de código fuente.

9. Sistemas de Correlación de Eventos

Sistema que combina toda la información de las diferentes herramientas de seguridad para mostrar por medio de la correlación de eventos qué sucede en la red en tiempo real, lo que le permite al supervisor tomar medidas con carácter proactivo ante un evento o incidente de seguridad.

Los sistemas de correlación de eventos permiten entre otras funciones:

a) Conocer exactamente lo que sucede en toda la infraestructura con la correlación de eventos entre dispositivos que se realiza en memoria y por lo tanto en tiempo real;
b) la correlación de eventos no lineal para que no sea necesario crear reglas para cada evento;
c) solucionar problemas de rendimiento mediante la comprensión de la relación entre las diferentes actividades de la infraestructura y los eventos que suceden;
d) explorar los datos de forma visual a través de una interfaz para una mejor comprensión;
e) realizar el análisis forense de eventos; y
f) tomar acciones de inmediato, tales como poner en cuarentena las máquinas infectadas, bloqueo de direcciones IP, deshabilitar cuentas de usuario, eliminar procesos no autorizados, reiniciar servicios, entre otros, para mitigar los ataques o incidentes de seguridad.

GOC-2019-554-O45
RESOLUCIÓN 127

POR CUANTO: El Acuerdo 8151, de 22 de mayo de 2017, del Consejo de Ministros, en su numeral Cuarto, apartado Primero, dispone que el Ministerio de Comunicaciones tiene como función específica, la de ordenar, regular y controlar los servicios de telecomunicaciones, informáticos y postales, nacionales e internacionales, la gestión de los recursos comunes y limitados en materia de dichos servicios y su implementación.

POR CUANTO: Las resoluciones 55 y 104 del Ministro de la Informática y las Comunicaciones, actualmente de Comunicaciones, de 9 de marzo de 2009 y de 16 de junio del 2011, respectivamente, regulan la organización, el funcionamiento, registro y expedición de licencias de operación para los proveedores de servicios públicos de Alojamiento, Hospedaje y Aplicaciones, y con las exigencias del desarrollo alcanzado en las Tecnologías de la Información y la Comunicación, los servicios y el uso racional de los recursos, se hace necesario actualizar las referidas normas jurídicas y en consecuencia derogar estas.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d), de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO DEL PROVEEDOR DE SERVICIOS PÚBLICOS DE ALOJAMIENTO Y DE HOSPEDAJE EN EL ENTORNO INTERNET

CAPÍTULO I

OBJETO, DEFINICIONES Y ALCANCE

Artículo 1. El objeto del presente Reglamento es establecer las normas para la organización, funcionamiento y expedición de licencias de operación del proveedor de servicios públicos de alojamiento y de hospedaje en el entorno Internet en el territorio nacional.

Artículo 2. El presente Reglamento se aplica a la persona jurídica que haya solicitado y reciba la licencia de operación del Ministerio de Comunicaciones, para brindar los servicios de alojamiento o de hospedaje o ambos.

Artículo 3. El proveedor de servicios públicos de alojamiento y de hospedaje en el entorno Internet, en lo adelante el proveedor, puede prestar servicios clasificados como:

a) De alojamiento, gestión y colocación de servidores;
b) de hospedaje de sitios, aplicaciones e información.

Artículo 4. El proveedor soporta sus servicios con alcance nacional e internacional sobre las redes públicas de telecomunicaciones, en correspondencia con la legislación vigente.

CAPÍTULO II
DE LA LICENCIA DE OPERACIÓN

Artículo 5. La condición de proveedor se otorga mediante aprobación y expedición de la licencia de operación, para lo que el aspirante realiza la solicitud a la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico del Ministerio de Comunicaciones, en lo adelante UPTCER.

Artículo 6. La UPTCER es la encargada de la expedición, modificación o renovación de la licencia de operación de proveedor y su inscripción en el Control Administrativo Central Interno del Ministerio de Comunicaciones; para las solicitudes que reúnan los requisitos establecidos y sean aceptadas, la UPTCER dispone de hasta treinta días hábiles a los fines de entregar la licencia de operación e igual plazo para notificar a los no aceptados.

Artículo 7. Se exceptúan de realizar la solicitud al Ministerio de Comunicaciones aquellos proveedores designados para prestar servicios públicos de acceso a Internet y los que se hayan autorizado por este Ministerio como proveedores públicos de alojamiento, hospedaje y aplicaciones, con anterioridad a la fecha de aprobación de este Reglamento.

Artículo 8. La solicitud debe ir acompañada de los documentos siguientes:

a) Carta del aspirante en la que se declare los datos generales de la entidad;
b) copia certificada del poder o resolución de designación del representante legal de la entidad;
c) documento que informe los aspectos técnicos del servicio, el equipamiento disponible y los programas y aplicaciones informáticas que utiliza;
d) dictamen sobre la seguridad de las Tecnologías de la Informacióny la Comunicación; y
e) otros documentos de interés que se soliciten por la UPTCER como requisito adicional a lo regulado por el presente Reglamento.

Los datos declarados en los documentos presentados pueden ser objeto de comprobación por los inspectores de las oficinas territoriales de Control del Ministerio de Comunicaciones.

Artículo 9. A partir de la solicitud presentada, la UPTCER entrega, de acuerdo con la condición otorgada los documentos siguientes:

a) Una licencia de operación, si fuere el solicitante un nuevo proveedor de servicios;
b) una modificación o renovación de la licencia de operación, si ya se le hubiere otorgado tal condición.

Artículo 10.1. La licencia de operación tiene un plazo de vigencia de cinco años; cualquier modificación en los parámetros informados en el Control Administrativo Central Interno del Ministerio de Comunicaciones, se comunica a la UPTCER por el representante legal de la entidad;

2. En la licencia de operación que se entregue se determina su nuevo término de duración, sobre la base de los datos aportados en las solicitudes de modificación.

Artículo 11. La licencia de operación se renueva dentro de los sesenta días antes del vencimiento del plazo de vigencia, mediante la presentación del documento de solicitud de renovación; una vez vencido el plazo de autorización, la entidad no puede brindar el servicio, y su representante legal está obligado a realizar todos los trámites como una nueva solicitud.

Artículo 12. El proveedor presenta la renuncia a su condición por escrito ante la UPTCER, con noventa días de antelación a la fecha en que se pretende que surta efectos.

Artículo 13. Constituyen causas para cancelar la licencia de operación por parte de la UPTCER, las siguientes:

a) El vencimiento del plazo por el que fue otorgada la licencia sin haberse solicitado su renovación;
b) el incumplimiento de lo establecido en el presente Reglamento, la legislación sobre telecomunicaciones, y las relacionadas con los servicios sobre internet y su seguridad;
c) la renuncia por parte del proveedor;
d) la extinción de la entidad a la que se le otorgó la licencia;
e) la cesión o el gravamen a favor de un tercero, en todo o en parte,de los derechos que son objeto de la licencia de operación otorgada; y
f) las demás que correspondan, según la legislación vigente.

Artículo 14. Los proveedores abonan por los derechos de licencia de operación de los servicios la cantidad de trescientos pesos cubanos por la licencia, y ciento cincuenta pesos cubanos por la renovación o modificación; el pago se realiza directamente en la sucursal bancaria según establece la legislación vigente del Ministerio de Finanzas y Precios y presentan el comprobante de pago a la UPTCER para la obtención de la licencia, quien anexa la copia de este al expediente.

CAPÍTULO III
DE LAS NORMAS TÉCNICAS, LA HOMOLOGACIÓN Y LOS ACUERDOS DE NIVEL DE SERVICIOS

Artículo 15. Las normas técnicas aplicables a la infraestructura sobre la que se soportan los servicios de un proveedor son las establecidas de acuerdo con la legislación vigente, de conformidad con las recomendaciones de la Unión Internacional de Telecomunicaciones o de otros organismos internacionales, y de los tratados de los que la República de Cuba sea Estado parte.

Artículo 16. El proveedor está obligado a cumplir las especificaciones de los puntos de conexión de los servicios de soporte que utilice; las interfaces entre los puntos de interconexión y la red del proveedor están normalizadas y se procura, siempre que sea posible, utilizar las más avanzadas técnicamente.

Artículo 17. Los equipos que se conecten a las redes públicas de telecomunicaciones o hagan uso del espectro radioeléctrico para la prestación del servicio, deben estar homologados según lo establecido y cumplir las disposiciones vigentes sobre el empleo del espectro radioeléctrico en el país.

Artículo 18. Los proveedores establecen en sus contratos con los proveedores de servicios de red, los indicadores de calidad que definan y garanticen los parámetros de estos, el cumplimiento de las recomendaciones internacionales y las regulaciones nacionales vigentes, así como aquellas que las partes acuerden complementariamente.

Artículo 19. Las partes acuerdan según las regulaciones vigentes, entre otros indicadores y parámetros de calidad de servicio, los siguientes:

a) Los tipos de medición de los niveles de calidad que hacen de manera independiente y la periodicidad de la medición de cada indicador;
b) las condiciones bajo las cuales existe intercambio de información sobre estos indicadores;
c) los medios empleados para el intercambio de la información;
d) los períodos dentro de los cuales se acepta por la otra parte la calificación que se haga de los mencionados niveles de servicio.

CAPÍTULO IV

DE LAS OBLIGACIONES DE LOS PROVEEDORES

Artículo 20. El proveedor al prestar servicios de alojamiento y de hospedaje garantiza las condiciones técnicas mínimas siguientes:
a) Sistema de almacenamiento conectado a la red, conocido como SAN;
b) local con condiciones apropiadas;
c) sistema de climatización redundante;
d) alimentación eléctrica estable, confiable y permanente;
e) grupo electrógeno de respaldo de energía;
f) sistema de detección de incendios;
g) sistema de aterramiento;
h) sistemas de seguridad física y lógica;
i) control de acceso al servicio;
j) monitorización sistemática;
k) registro bajo el dominio.cu en el CUBANIC;
l) sistema de respaldo de la información, backup, y de recuperación ante desastres.

Artículo 21. El proveedor tiene las obligaciones siguientes:
a) Utilizar los servicios portadores, finales o de difusión existentes en la red pública de telecomunicaciones, sin vulnerar las concesiones administrativas otorgadas de servicios públicos de telecomunicaciones;
b) admitir como clientes del servicio a todas las personas naturales o jurídicas que lo deseen, siempre que tenga capacidades disponibles;
c) garantizar la administración, operación y seguridad de la información de los servicios que presta, de acuerdo con lo establecido en el marco jurídico existente;
d) adoptar las medidas necesarias para garantizar el cumplimiento de los principios de:
   i. salvaguarda del orden público y la defensa del país;
   ii. no discriminación; y
   iii. protección de la juventud y de la infancia.
e) garantizar, en lo que le corresponde, la seguridad de las Tecnologías de la Información y la Comunicación en la red que utilice;
f) adquirir tecnología que permita el empleo de técnicas de virtualización para la optimización y uso eficiente de los recursos disponibles y brindar servicios soportados en la nube;
g) cumplir los requisitos técnicos del servicio que le sirve de soporte, incluidos los puntos de conexión, así como lo estipulado en las condiciones de interconexión contenidas en el Reglamento correspondiente y para el uso del espectro radioeléctrico;
h) sistematizar la gestión de vulnerabilidades, versiones y actualizaciones, parches, de las aplicaciones, software y firmware, sobre la base de la publicación de alertas de los fabricantes y la vigilancia tecnológica;

i) implementar las medidas y herramientas que garanticen la seguridad de las infraestructuras de la red y la detección e investigación de incidentes de seguridad;
j) cumplir las disposiciones establecidas por los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, ante situaciones excepcionales;
k) reportar los incidentes de seguridad informática que se detecten por las vías y procedimientos establecidos en la legislación vigente;
l) cumplir con calidad el servicio contratado con sus clientes;
m) brindar en línea a sus clientes, la información sobre el uso de los servicios;
n) mantener informados a los clientes de las características, bondades, tarifas a aplicar y otras cuestiones relacionadas con el servicio ofertado; detallar las características y alcance del servicio que presta en los contratos a suscribir y comunicar cualquier modificación de este con una antelación de treinta días;
o) mantener el principio de inviolabilidad y secreto de las comunicaciones y de confidencialidad de los aspectos requeridos, de conformidad con lo dispuesto en la Constitución de la República y las normas dictadas al efecto;
p) establecer un sistema eficiente de recepción y solución de reclamaciones y quejas de los clientes por los servicios proporcionados;
q) permitir y facilitar la realización de inspecciones de los equipos, edificios e instalaciones relacionadas con el servicio autorizado que se indiquen por las oficinas territoriales de Control, por la Oficina de Seguridad para las Redes Informáticas ambas del Ministerio de Comunicaciones y por los demás órganos e instancias autorizados del país, sobre los documentos y los servicios en operación y el acceso a los equipos e instalaciones;
r) brindar las informaciones establecidas u otras que se solicite por el Ministerio de Comunicaciones;
s) garantizar a sus clientes de forma fácil la administración de los servicios contratados que lo requieran;
t) establecer en los contratos de servicios la exigencia del mantenimiento y soporte de las aplicaciones y servicios hospedados;
u) cumplir con la protección y tratamiento de los datos personales de sus clientes;
v) potenciar la capacitación del personal especializado que labora en esta área;
w) solicitar la licencia de proveedor de servicios públicos de aplicaciones a las personas que requieran este servicio de hospedaje;
x) priorizar los servicios de alojamiento a los sitios web a través de los cuales se brinden servicios públicos de información o de aplicaciones, entre los que se incluyen los sitios oficiales de los órganos del Estado y los organismos de la Administración Central del Estado, los proyectos nacionales de informatización y otros de interés nacional aprobados por el Ministerio de Comunicaciones.

Artículo 22. El proveedor cuando tenga conocimiento efectivo de acuerdo con lo dispuesto en el Artículo 25 de actividades ilegales o que violen los principios enunciados en el inciso d) del artículo anterior, está obligado a informar a las autoridades competentes y actuar con diligencia para evitar o poner fin a tales actividades.

Artículo 23. El proveedor cuando detecte vulnerabilidades que afectan la seguridad de la infraestructura tecnológica o que puedan propiciar la afectación de otros clientes hospedados o alojados por el propio proveedor, o de la infraestructura de terceros países, debe gestionar su solución y, en dependencia del impacto, resolver el contrato con el cliente que la origina e informar a las autoridades competentes.

Artículo 24. El proveedor de un servicio consistente en almacenar contenidos de información que proporciona y actualiza el propio cliente, no es responsable por la información almacenada, siempre que:

a) No tenga conocimiento efectivo de que la actividad o la información almacenada es ilícita, violatoria de un principio, o de que lesiona bienes o derechos de un tercero susceptibles de indemnización; o que se demuestre la reclamación de la legitimidad de la violación del derecho de propiedad de algún artículo publicado en su sitio;
b) con el conocimiento efectivo de los hechos, actúe con diligencia para retirar la información o hacer imposible el acceso a ella, y poner en conocimiento de esta actuación al cliente del servicio de que se trate.

Artículo 25. El proveedor de servicios tiene conocimiento efectivo de que la actividad o la información almacenada es ilícita, violatoria de un principio, o que lesiona bienes o derechos de un tercero susceptibles de indemnización, cuando:

a) Un órgano competente haya declarado la ilicitud de los datos, orientado su retirada o que se imposibilite el acceso a estos;
b) haya recibido informe sobre la existencia de una infracción del marco regulatorio vigente.

Artículo 26. El proveedor es responsable de la información almacenada en su infraestructura cuando el cliente del servicio le contrate la gestión de esta.

Artículo 27. Los proveedores son responsables de coordinar entre sí la interconexión, sincronización y redundancia de sus centros de datos con el objetivo de garantizar la estabilidad y continuidad de los servicios.

CAPÍTULO V
DE LAS TARIFAS PARA LOS SERVICIOS

Artículo 28. El proveedor establece las tarifas de los servicios públicos de alojamiento y de hospedaje de conformidad con la legislación vigente en el país.

Artículo 29. El proveedor establece precios preferenciales en el pago de sus servicios, cuando los clientes hospedan proyectos de impacto nacional en la estrategia de informatización, determinados por la Dirección General de Informática.

CAPÍTULO VI
MEDIDAS Y PROCEDIMIENTOS A APLICAR ANTE INCUMPLIMIENTOS DEL PROVEEDOR

Artículo 30. El proveedor que incumpla lo dispuesto en el presente Reglamento y en las disposiciones legales vigentes en la materia, está sujeto a la aplicación de las medidas siguientes:

a) Notificación preventiva;
b) invalidación temporal o parcial o cancelación de las licencias de operación administrativamente entregadas por la UPTCER del Ministerio de Comunicaciones;
c) suspensión temporal o parcial o cancelación de los servicios que haya contratado con el proveedor de servicios públicos de transmisión de datos y acceso a Internet.

Artículo 31. El inspector de las oficinas territoriales de Control del Ministerio de Comunicaciones es la autoridad facultada para aplicar las medidas referidas en el artículo anterior e informar a la UPTCER sobre estas y la decisión acerca de su aplicación.

Artículo 32. El proveedor sujeto a la aplicación de las medidas descritas en el Artículo 30, puede apelar en primera instancia ante el Director de las oficinas territoriales de Control, en el plazo de diez días hábiles contados a partir de la fecha de su notificación, formular las alegaciones que considere oportunas y ofrecer las pruebas que estime convenientes; el Director de las oficinas territoriales de Control dispone de un plazo de treinta días hábiles para dar respuesta a partir de la presentación de la apelación.

Artículo 33. El proveedor que decida impugnar la medida impuesta en la primera instancia de reclamación, dispone de un plazo de diez días hábiles a partir de su notificación para solicitar una revisión ante el Director General de Informática, el que dispone de un plazo de treinta días hábiles, contados a partir del recibo oficial de la reclamación, para resolver lo que proceda; contra esta decisión no cabe otro recurso por vía administrativa.

Artículo 34. El proveedor que haya sido objeto de una medida por incumplimiento de sus obligaciones, una vez resuelto el expediente que dio lugar a esta, puede presentar una nueva solicitud de licencia de operación a la UPTCER, quien tiene en cuenta la información presentada y, una vez comprobada por los inspectores de las oficinas territoriales de Control la solución de las deficiencias detectadas, determina sobre el otorgamiento de la licencia.

SEGUNDO: El proveedor para solicitar, mantener o ampliar los servicios de conectividad presenta su licencia de operación al operador de servicios públicos de telecomunicaciones.

TERCERO: El Director General de la UPTCER queda responsabilizado con la elaboración de los procedimientos internos necesarios para el otorgamiento, renovación o modificación de las licencias de operación vigentes a la fecha de entrada en vigor de la presente.

DISPOSICIÓN FINAL

PRIMERA: Los proveedores de servicios públicos de alojamiento, hospedaje y aplicaciones, en un plazo de noventa días posteriores a la entrada en vigor de la presente, actualizan la información relativa a los parámetros de prestación del servicio, de acuerdo con lo que se dispone en este Reglamento, para su inscripción en el Control Administrativo Central Interno y que le sea entregada por la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico la licencia de operación como proveedor de servicios públicos de alojamiento y hospedaje.

SEGUNDA: Los directores generales de Informática, de Comunicaciones y de la UPTCER, y los directores de Inspección y de las oficinas territoriales de control del Ministerio de Comunicaciones, quedan encargados, según corresponda, del control del cumplimiento de lo que por la presente se dispone.

TERCERA: El glosario de términos y definiciones anexo forma parte del contenido de la presente Resolución.

CUARTA: Derogar las resoluciones 55, de 9 de marzo de 2009 y 104, de 16 de junio de 2011 del Ministro de la Informática y las Comunicaciones.

NOTIFÍQUESE a los directores generales de Informática, de Comunicaciones, y de la Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico y a los directores territoriales de control pertenecientes a este Ministerio, al Presidente Ejecutivo de la Empresa de Telecomunicaciones de Cuba, S.A., al Presidente del Grupo Empresarial de la Informática y las Comunicaciones y a los proveedores públicos de alojamiento, hospedaje y aplicaciones.

COMUNÍQUESE a los viceministros, a los directores de Inspección y de Regulaciones, al Director General de la Oficina de Seguridad para las Redes Informáticas, todos del Ministerio de Comunicaciones, así como a cuantas personas naturales y jurídicas deban conocerla.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO

GLOSARIO DE TÉRMINOS Y DEFINICIONES

1. **Almacenamiento Conectado a la Red (SAN del inglés Storage Area Networks)**: Capacidad de almacenamiento extra que puede solicitar un cliente que tiene un contrato de servidor dedicado, es decir, un servidor para su uso exclusivo, además puede ser empleado como complemento de otros servicios que se comercialicen.
2. **Alojamiento**: Servicio de colocación, conexión, gestión y administración de equipos informáticos, consistente básicamente en vender o alquilar un espacio físico de un centro de datos, para que el cliente coloque su propio equipamiento.
3. **Hospedaje**: Servicio de almacenamiento, conectividad y otros servicios dedicados al despliegue de la información que se quiera sea accesible por una red, que pueden ser desde un sitio de Internet, programas y las aplicaciones asociadas hasta la información de una red interna o Intranet.
4. **Licencia de operación:** Autorización por la que se faculta a su tenedor para la operación de los servicios de alojamiento y hospedaje.
5. **Proveedor de servicios públicos de Aplicaciones:** Persona jurídica o natural autorizada para comercializar servicios de aplicaciones a terceros y hace uso del entorno Internet, conocidos como ASP, por sus siglas en inglés.
6. **Proveedor de servicios públicos de acceso a Internet:** Persona jurídica autorizada para prestar uno o varios tipos de servicios del entorno Internet, en todo el territorio nacional, conocidos como ISP, por sus siglas en inglés.

GOC-2019-555-O45

RESOLUCIÓN 128

POR CUANTO: El Decreto 360 “Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional”, de 5 de junio de 2019 en su Disposición Final Primera establece, que los jefes de los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales y los órganos del Poder Popular, en el marco de su competencia, dictan las disposiciones legales, realizan el control y fiscalización, y establecen las coordinaciones que resulten necesarias relativas a la aplicación del referido Decreto.

POR CUANTO: A partir de la experiencia acumulada en la aplicación de las Resoluciones 127 del Ministro de la Informática y las Comunicaciones, que aprobó el Reglamento de Seguridad de las Tecnologías de la Información, de 24 de julio de 2007 y la 192, de 20 de marzo de 2014, del Ministro de Comunicaciones, que puso en vigor el Reglamento para contrarrestar el envío de mensajes masivos dañinos a través de las redes de telecomunicaciones; resulta necesario emitir una nueva disposición normativa que actualice el contenido normativo de las referidas disposiciones, para atemperarlas a las exigencias del proceso de informatización de la sociedad y en consecuencia proceder a su derogación.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el siguiente:

REGLAMENTO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. El presente Reglamento tiene por objeto complementar las disposiciones del Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional"de 5 de junio de 2019, y establecer las funciones de los sujetos que intervienen en esta, así como garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país.

Artículo 2. Este Reglamento es de aplicación a los órganos, organismos de la Administración Central del Estado, el Banco Central de Cuba, las entidades nacionales, los órganos del Poder Popular, el sistema empresarial y las unidades presupuestadas, las formas de propiedad y gestión no estatal, las empresas mixtas, las formas asociativas sin ánimos de lucro, las organizaciones políticas, sociales y de masas y las personas naturales, en lo adelante la entidad.

CAPÍTULO II
DEL SISTEMA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 3. El Sistema de Seguridad de las Tecnologías de la Información y la Comunicación tiene como objetivo minimizar los riesgos sobre los sistemas informáticos y garantizar la continuidad de los procesos informáticos.

Artículo 4. Las formas de propiedad y gestión no estatal y las personas naturales, cumplen lo dispuesto en el presente Reglamento, en lo que corresponda, aunque no cuenten con el personal especializado.

Artículo 5. El jefe de la entidad a cada nivel es el máximo responsable de la seguridad de las Tecnologías de la Información y la Comunicación, en lo adelante seguridad de las TIC, en su organización, y garantiza la actualización de los Planes de Seguridad de las TIC y considera para ello los factores siguientes:

a) La aparición de nuevas vulnerabilidades;
b) los efectos de los cambios de tecnología o de personal;
c) la efectividad del sistema, demostrada por la naturaleza, número y daño ocasionado por los incidentes de seguridad registrados.

Artículo 6. Los especialistas en seguridad de las TIC a cada nivel, cumplen las funciones siguientes:

a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad de las TIC, supervisar su aplicación y disciplina en su cumplimiento;
b) establecer y mantener los controles, en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado;
c) participar en la evaluación de riesgos y vulnerabilidades de su entidad;
d) controlar y supervisar la disponibilidad de los bienes informáticos;
e) asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las TIC;
f) establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software, sin la autorización de la dirección de la entidad;
g) participar en la elaboración de los procedimientos de recuperación, ante incidentes de seguridad y en sus pruebas periódicas;
h) informar a los usuarios de las regulaciones establecidas.

Artículo 7. Los responsables de la seguridad de las TIC a cada nivel, responden por la protección de los bienes informáticos que le han sido asignados y tienen los deberes siguientes:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios y la vigencia de estos accesos;
b) participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad de las TIC en la parte que concierne a su esfera de acción y garantizar su cumplimiento;
c) participar en la evaluación de riesgos y vulnerabilidades de su entidad;
d) aplicar las medidas y procedimientos establecidos en su área de responsabilidad;
e) especificar al personal subordinado, las medidas y procedimientos establecidos y controlar su cumplimiento;
f) participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas;
g) imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

Artículo 8. Los usuarios de las TIC en sus entidades, tienen los deberes siguientes:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad de las TIC imprescindibles para el desempeño de su trabajo;
b) contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos;
c) cumplir las medidas de seguridad establecidas;
d) proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usar la información que contiene o utilizar de manera impropia el sistema al que esté conectado;
e) contar con la autorización del jefe facultado para instalar o utilizar en las tecnologías, equipamientos, o programas, o modificar su configuración;
f) cumplir las reglas establecidas para el empleo de las contraseñas;
g) informar al dirigente facultado de cualquier anomalía de seguridad detectada.

CAPÍTULO III

DEL EMPLEO SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

SECCIÓN PRIMERA

Bienes informáticos

Artículo 9. Los bienes informáticos están bajo la custodia documentada legalmente de la persona designada para hacer uso del bien, quien es responsable de su protección.

Artículo 10. El jefe de la entidad instrumenta los procedimientos que se requieran para garantizar la autorización y el control sobre la utilización y movimiento de los bienes informáticos.

Artículo 11. El jefe del área o unidad organizativa que atiende las TIC define el procedimiento de uso de empleo y responsabilidad de los bienes informáticos que son móviles (portátiles o removibles), para las personas que utilizan estos bienes dentro y fuera de la entidad, que incluye:

a) Comunicar de inmediato por el ususario a la dirección de la entidad la pérdida o extravío del bien;

b) no contener datos importantes e información sensible, cuando se extraigan de la entidad, y tener implementadas medidas de protección;
c) no conservar datos personales o sobre la entidad a través de los que se pueda acceder a sus sistemas.

SECCIÓN SEGUNDA

De la Dirección del personal

Artículo 12. Las funciones y responsabilidades de seguridad de las TIC, tanto generales como específicas, son debidamente documentadas e incluidas dentro de las responsabilidades laborales del personal de la entidad.

Artículo 13. El jefe del área o unidad organizativa que atiende las TIC de la entidad está obligado a preparar y exigir responsabilidad al trabajador en materia de seguridad de las TIC, así como a aplicar las sanciones en caso de que este incumpla los requerimientos establecidos.

Artículo 14. La dirección de cada entidad establece previamente la utilización de las TIC y sus servicios asociados conforme a la necesidad de uso en interés de la propia entidad.

Artículo 15. La introducción, ejecución, distribución o conservación de programas en los medios de cómputo que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, solo se efectúan por las personas debidamente autorizadas por el jefe del área o unidad organizativa que atiende las TIC; se excluye el uso de aplicaciones destinadas a la comprobación de los sistemas instalados en la organización para el control interno de las operaciones realizadas y en ningún caso, este tipo de programas o información se expone mediante las TIC para su libre acceso.

SECCIÓN TERCERA

Seguridad Física

Artículo 16. En los edificios e instalaciones de cada entidad, su dirección determina las áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido, en dependencia de la importancia de los bienes informáticos que contiene y su utilización de acuerdo con la denominación siguiente:

a) **Áreas limitadas:** en las que se concentran bienes informáticos de valor medio, cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.
b) **Áreas restringidas:**donde se concentran bienes informáticos de alto valor e importancia crítica, cuya afectación pueda paralizar o afectar severamente la gestión de sectores de la economía o de la sociedad; territorios o entidades.
c) **Áreas estratégicas:** en las cuales se concentran bienes informáticos de alto valor e importancia crítica, que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública, y el suministro de agua u otra que por su importancia se considere necesaria.

Artículo 17. Las áreas o zonas controladas se protegen para garantizar el acceso exclusivamente al personal autorizado y la dirección de la entidad establece las medidas que correspondan.

Artículo 18. En la selección y diseño de las áreas controladas se tiene en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

Artículo 19. El equipamiento instalado en las áreas controladas se protege contra fallas de alimentación y otras anomalías eléctricas, lo que incluye el uso de fuentes de alimentación alternativas para los procesos que deben continuar en caso de un fallo de electricidad prolongado, así como se ubica y protege de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

Artículo 20. En las áreas limitadas se aplican las medidas de protección física siguientes:

a) Seleccionar para su ubicación locales cuyas puertas y ventanas estén provistas de cierres seguros;
b) aplicar medidas que garanticen su seguridad y eviten la visibilidad hacia el interior de los locales con ventanas que se comuniquen al exterior de la instalación;
c) prohibir el acceso de personal no autorizado por la dirección de la entidad;
d) permitir la permanencia del personal fuera del horario laboral con la debida justificación y autorización por escrito de la dirección de la entidad; las autorizaciones referidas se conservan por un término mínimo de seis meses.

Artículo 21. En las áreas restringidas además de las medidas requeridas en las áreas limitadas, se aplican las siguientes:

a) Se mantienen cerradas incluso cuando permanezcan personas laborando, y el acceso se controla mediante los registros que para ello se establezcan;
b) establecer por la entidad requisitos de idoneidad, al personal que accede a estas áreas;
c) utilizar sistemas de detección y alarma que permitan una respuesta efectiva ante accesos no autorizados, cuando no se encuentre el personal que en ellas labora;
d) implementar mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas;
e) prohibir la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad; así como de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a esta.

Artículo 22. En las áreas estratégicas además de las medidas requeridas en las áreas restringidas y limitadas, se aplican las siguientes:

a) Establecer una identificación individual que especifique las áreas de trabajo para el personal que labore o que por razones de servicio sea autorizado a permanecer en estas; la cual debe llevarse por cada trabajador en un lugar visible;
b) implementar medios especiales de supervisión de la actividad que en ellas se realiza;
c) el acceso por personas ajenas solo se autoriza de manera excepcional, restringida y bajo supervisión, mediante un permiso especial, emitido por la dirección de la entidad, el que se conserva por un término mínimo de seis meses.

Artículo 23. Los recursos relacionado con las TIC, independientemente de su importancia, se protegen contra alteraciones o sustracciones, ya sea de estas, de sus componentes o de la información que contienen.

Artículo 24. El jefe de la entidad es el responsable de que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante, con el fin de asegurar su disponibilidad e integridad; en caso de necesidad de envío del equipamiento fuera de las instalaciones para que reciban mantenimiento, este se realiza en correspondencia con los procedimientos establecidos por la dirección de la entidad a tales efectos, según las regulaciones vigentes en el país en materia de protección de la información.

Artículo 25. El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información se autoriza por su dirección, mediante el documento correspondiente; la seguridad que se le garantice por el autorizado tiene que ser equivalente a la establecida en las instalaciones habituales del equipamiento usado para este propósito.

Artículo 26. El equipamiento antes de causar baja o ser destinado a otras funciones, se le aplica el procedimiento de borrado seguro, para evitar que la información que contiene pueda resultar comprometida; los dispositivos de almacenamiento que contengan información crítica para la entidad son destruidos físicamente.

Artículo 27. Se prohíbe el movimiento de los equipos de la entidad y de los programas y aplicaciones informáticas sin la autorización escrita del jefe facultado; en caso de que se autorice se registra el movimiento a la salida del medio y a su entrada al reintegrarse a su origen; así como se realizan los controles sorpresivos para detectar las extracciones no autorizadas.

CAPÍTULO IV
SEGURIDAD DE LAS OPERACIONES

Artículo 28. Las acciones para cubrir las brechas de seguridad y la corrección de los errores de los sistemas y aplicaciones son minuciosamente controladas en cada entidad, por sus respectivos jefes; los procedimientos aseguran en lo fundamental que:

a) Sean eliminadas o minimizadas las vulnerabilidades conocidas;
b) solo el personal identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos;
c) todas las acciones de emergencia tomadas sean documentadas detalladamente;
d) la acción de emergencia sea reportada a la dirección de la entidad y realizada de manera ordenada.

Artículo 29. En caso de ser necesario compartir recursos a través de la red, se define, por la persona autorizada, de forma precisa con los usuarios se hará, el nivel de acceso y la duración del intercambio.

Artículo 30. En el uso de credenciales de acceso, cuya contraseña es textual, como método de autenticación de usuarios, se cumplen los requisitos siguientes:

a) Ser privadas e intransferibles;
b) su estructura, fortaleza y frecuencia de cambio se corresponden con el riesgo estimado para el acceso que protegen, implementado a través de mecanismos automatizados de validación;
c) la composición de los caracteres es alfanumérica (letras, números y símbolos) sin un significado trivial, con una longitud mínima de 8 caracteres;
d) no pueden ser visualizadas en pantalla mientras se teclean;
e) no se almacenan en texto claro, sin cifrar, ni son recordadas en ningún tipo de terminal.

Artículo 31. En el caso de mecanismos de autenticación diferentes al mencionado anteriormente, se cumple las normas de seguridad establecidas para estos.

Artículo 32. El jefe de la entidad apueba los derechos y privilegios de acceso a sistemas y datos que tiene cada usuario, asi como el procedimiento escrito en cada caso para otorgar o suspender estos accesos.

Artículo 33. Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procede al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, y se preserva para su posterior análisis y descontaminación por personal especializado; además, se revisan los soportes con los que haya interactuado el medio contaminado.

Artículo 34. La contaminación por programas malignos se considera un incidente de seguridad y se cumple en este caso lo establecido en el Artículo 48 del presente Reglamento; en todos los casos se tiene que determinar el origen y la responsabilidad de las personas involucradas.

Artículo 35. El usuario que a través de sus equipos terminales de telecomunicaciones reciba mensajes masivos dañinos, tiene el derecho de presentar a su operador o proveedor una queja con las pruebas relativas de los hechos ocurridos; al que le corresponde tomar las medidas que procedan para eliminar la situación surgida.

CAPÍTULO V
SEGURIDAD DE LAS REDES

Artículo 36. El administrador de una red informática tiene, en relación con la seguridad de las TIC, los deberes siguientes:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red;
b) realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red;
c) garantizar que los servicios implementados sean utilizados para los fines que fueron creados;
d) comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes;
e) activar los mecanismos técnicos y organizativos de respuesta ante distintos tipos de incidentes y acciones nocivas que se identifiquen, y preservar toda la información requerida para su esclarecimiento;
f) participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas;
g) informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento;
h) garantizar que en el registro de trazas se incluya las relacionadas con la navegación a Internet, que permitan correlacionar la dirección IP real de salida al proveedor de servicios de Internet, con las IP privadas empleadas en las redes internas de la entidad;
i) participar en la confección y actualización del Plan de Seguridad de las TIC;
j) implementar y operar los controles que se establezcan para gestionar los riesgos de seguridad.

Artículo 37. En el empleo de las redes inalámbricas se tienen en cuenta, además de los aspectos de su seguridad, los siguientes:

a) Contar con la autorización, a través del procedimiento establecido, de la entidad facultada para su despliegue y explotación;
b) utilizar protocolos de cifrado de datos aprobados para la red de telecomunicaciones inalámbrica que lo requiera;
c) utilizar filtrado de direcciones MAC (conocida como Media Access Control) cuando sea posible y no se afecten los servicios para la que están destinadas;
d) configurar la potencia de irradiación al nivel establecido por la autoridad facultada a esos efectos.

Artículo 38. El jefe de la entidad orienta la ejecución de procedimientos periódicos de verificación de la seguridad de las redes, con el fin de detectar posibles vulnerabilidades, incluye para ello, cuando sea procedente, la comprobación de forma remota por entidades facultadas oficialmente, debido a la sensibilidad de estas acciones.

Artículo 39. En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos, se implementan mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

Artículo 40. En los casos de redes corporativas que prevean la extrapolación de servicios internos, la conexión se realiza por puertos bien identificados y mediante la protección con dispositivos que garanticen el acceso a esos servicios por el personal autorizado.

Artículo 41. Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas, solo se utilizan en interés de esta; la asignación de cuentas para su empleo se aprueba, en todos los casos, por la dirección de la entidad, sobre la base de las necesidades requeridas para su funcionamiento.

Artículo 42. Los servicios ofrecidos al público que son autorizados a una entidad específica, no forman parte de la red corporativa.

Artículo 43. La configuración del servicio de correo electrónico tiene que garantizar que solo el propietario de una cuenta pueda enviar y recibir mensajes desde esta.

Artículo 44. Se prohíbe vincular cuentas de correo electrónico de un servidor de una entidad a un servidor en el exterior del país, con el fin de redireccionar y acceder a los mensajes a través de este.

CAPÍTULO VI
DE LOS INCIDENTES DE SEGURIDAD

Artículo 45. La estrategia que se formule en la entidad ante cualquier incidente o violación de la seguridad es consecuente con sus objetivos básicos, donde se define el Plan de Prevención de Riesgos; además tiene en consideración:

a) Los riesgos que enfrenta en términos de probabilidad y su impacto, incluye una identificación y asignación de prioridades a los procesos críticos;
b) el impacto probable de las interrupciones sobre la gestión de la entidad;
c) la comprobación y actualización de manera periódica de los planes y procesos establecidos;
d) las acciones para la recuperación.

Artículo 46. Los procedimientos para la gestión de incidentes y violaciones de seguridad de las TIC, tienen los requisitos siguientes:

a) El reporte inmediato de la acción a la autoridad correspondiente;
b) la comunicación con los afectados o los involucrados en la recuperación del incidente;
c) el análisis y la identificación de las causas;
d) el registro de todos los eventos vinculados;
e) la recolección y preservación de las trazas de auditoría y otras evidencias;
f) la planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario.

Artículo 47. Ante cualquier incidente que afecte la seguridad de las TIC de una entidad, su dirección designa una comisión, integrada por especialistas no comprometidos directamente con este hecho, encargada de realizar las investigaciones necesarias para esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

Artículo 48. La dirección de cada entidad queda obligada, al producirse un incidente o violación de la seguridad informática, reportarlo inmediatamente a la Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones y a la instancia superior de la entidad; este reporte incluye:

a) En qué consistió el incidente o violación;
b) fecha y hora de comienzo del incidente y de su detección;
c) implicaciones y daños para la entidad y para terceros;
d) acciones iniciales tomadas;
e) evaluación preliminar.

CAPÍTULO VII

PRESTACIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA A TERCEROS

Artículo 49. La Dirección General de Informática del Ministerio de Comunicaciones es la unidad organizativa que autoriza las entidades que pueden brindar servicios de seguridad informática a terceros.

Artículo 50. Los requerimientos que cumple la entidad para solicitar la autorización que le permita prestar servicios de seguridad de las TIC a terceros, son los siguientes:
a) Que su objeto social se relacione con los servicios de las TIC;
b) que cuente con mecanismos que garanticen la calidad de los servicios y la idoneidad del personal;
c) preparación técnico-profesional de los especialistas que laboren en la entidad;
d) que esté en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;
e) que cuente con medios de protección de la información a la que tenga acceso durante su trabajo;
f) que los productos de seguridad informática utilizados, estén debidamente autorizados por las entidades facultadas;
g) que sea una entidad estatal cuyo personal resida de forma permanente en el país.

Artículo 51. Las entidades autorizadas por la Direccion General de Informática para brindar servicios de seguridad informática en las redes de otras entidades, están en la obligación de:
a) Mantener el máximo de discreción en relación con las posibles vulnerabilidades detectadas;
b) abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio propio;
c) informar a las entidades designadas para el control del ciberespacio, los resultados de las comprobaciones realizadas.

CAPÍTULO VIII

DE LA INSPECCIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Artículo 52. La inspección estatal a la seguridad de las TIC tiene como objetivos principales, los siguientes:
a) Evaluar los conocimientos y la aplicación de la base legal vigente;
b) realizar diagnósticos sobre la efectividad de los sistemas de seguridad informática aplicados en las entidades;
c)verificar el grado de control y supervisión que se ejerce sobre los bienes informáticos, así como los resultados de la gestión de la seguridad informática;
d) evaluar la efectividad de los planes de seguridad informática elaborados y su actualización y correspondencia con las necesidades de cada entidad;
e) valorar la gestión e influencia que ejercen las instancias superiores sobre esta actividad.

Artículo 53. Los inspectores de seguridad de las TIC tienen las facultades siguientes:

a) Realizar la inspección con o sin aviso previo;
b) evaluar el estado de cumplimiento y aplicación de la base legal de la Seguridad Informática vigente;
c) identificar las violaciones y vulnerabilidades detectadas en el Sistema de Seguridad Informática;
d) hacer evaluaciones, recomendaciones y disponer acciones correctivas ante violaciones de la base legal establecida;
e) proponer sanciones administrativas según las previstas en el Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional";
f) recomendar la realización de auditorías;
g) proponer la suspensión de los servicios, cuando se viole lo establecido en el presente Reglamento;
h) verificar el cumplimiento de las acciones correctivas que hayan sido aplicadas como resultado de inspecciones anteriores, si las hubiere;
i) exigir la entrega de las trazas o registros de auditoría de las TIC u otras posibles evidencias que se consideren necesarias;
j) ocupar para su revisión los medios informáticos involucrados en cualquier tipo de incidente de seguridad y proponer su decomiso definitivo a las instancias correspondientes.

DISPOSICIÓN ESPECIAL

ÚNICA: Se facultan a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, a adecuar para sus sistemas lo dispuesto en la presente Resolución.

DISPOSICIONES FINALES

PRIMERA: Se faculta al Director General de la Oficina de Seguridad las Redes Informáticas perteneciente a este Ministerio, para implementar las acciones que se requieran con el fin de dar cumplimiento a lo que por la presente se dispone.

SEGUNDA: El Viceministro que atiende la Informática en el Ministerio de las Comunicaciones, instrumenta las medidas que se requieran en el control de los parámetros que sean necesarios para la contención de los mensajes masivos dañinos.

TERCERA: Derogar las resoluciones 127 del Ministro de la Informática y las Comunicaciones, de 24 de julio de 2007 y la 192 del Ministro de Comunicaciones, de 20 de marzo de 2014.

NOTIFÍQUESE a los directores generales de Defensa y de la Oficina de Seguridad para las Redes Informáticas, a los directores territoriales de control, todos del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones, del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

GOC-2019-556-O45
RESOLUCIÓN 129

POR CUANTO: El Decreto 360 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional" de 5 de junio de 2019 establece en su Artículo 19 que el diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizan en correspondencia con las metodologías establecidas por el Ministerio de Comunicaciones, por lo que se considera necesario establecer la Metodología para la Gestión de la Seguridad Informática en todo el país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar la Metodología para la Gestión de la Seguridad Informática que se anexa y que forma parte integrante de la presente Resolución.

SEGUNDO: Las entidades disponen de ciento ochenta días contados a partir de la entrada en vigor de la presente Resolución, para establecer sus Sistemas de Gestión de la Seguridad Informática, en correspondencia con lo regulado en la referida metodología.

TERCERO: La Oficina de Seguridad para las Redes Informáticas del Ministerio de Comunicaciones es la encargada de ejercer el control del cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministros de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, la Metodología para la Gestión de la Seguridad Informática.

NOTIFÍQUESE al director general de la Oficina de Seguridad para las Redes Informáticas.

COMUNÍQUESE a los viceministros, al director general de Informática y al director de Regulaciones del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica de este Ministerio.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 días del mes de junio de 2019.

Jorge Luis Perdomo Di-Lella

ANEXO

METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

ÍNDICE

Objeto

La presente metodología tiene por objeto determinar las acciones a realizar en una entidad durante el diseño, la implementación y posterior operación de un Sistema de Gestión de la Seguridad Informática, en lo adelante SGSI, compuesta por dos partes, la primera se dedica al SGSI y la segunda a la estructura y contenido del Plan de Seguridad Informática. Constituye un complemento a lo exigido en el Decreto de Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional y el Reglamento de Seguridad para las Tecnologías de la Información y la Comunicación en cuanto a la obligación de diseñar, implantar y mantener actualizado un Sistema de Seguridad Informática, a partir de los bienes a proteger y de los riesgos a que están sometidos.

Alcance

Esta metodología está dirigida a todas las personas vinculadas con las Tecnologías de la Información y la Comunicación, en lo adelante TIC, de una entidad, ya sea por la responsabilidad que tienen asignadas en relación con los bienes informáticos o por los beneficios que de ellos obtienen.

Los primeros destinatarios de esta metodología son los directivos y funcionarios de los distintos niveles de una entidad, que responden por el buen funcionamiento de las tecnologías y la información que en ellas se procesa.

Términos y definiciones

A los efectos de la presente metodología se entiende por:

1. **Análisis de riesgos:** Proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos, e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.
2. **Identificación de usuarios:** Identificador (ID) que define quién es el usuario y qué lo identifica unívocamente en el sistema, diferenciándolo en los sistemas multiusuario del resto.
3. **Impacto:** Daño producido por la materialización de una amenaza.
4. **Riesgo residual:** Riesgo remanente después de aplicados controles de seguridad para minimizarlo.
5. **Sistema informático:** Conjunto de bienes informáticos de que dispone una entidad para su correcto funcionamiento y la consecución de sus objetivos.
6. **Soportes removibles:** Cualquier tipo de dispositivo intercambiable que permita la transferencia o almacenamiento de información.
7. **Trazas de auditoría:** Registros que se generan para describir la información asociada a eventos de interés en los diferentes procesos que se ejecutan en las TIC; están compuestos por secciones y campos donde se describen aspectos como fecha y hora, tipo de evento, quién o qué lo causa, y qué se afecta, que permiten comprender el evento que se registra y usualmente se registran en orden cronológico.

El SGSI de una entidad se diseña con la consideración del conjunto de sus bienes informáticos a partir de su importancia y el papel que representan para el cumplimiento de su actividad, por lo que se presta especial atención a aquellos que son críticos en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos.

Un SGSI conlleva la conformación de una estrategia sobre cómo tratar los aspectos de seguridad e implica la implementación de los controles necesarios para garantizar el cumplimiento de lo establecido en esta materia, a partir de un análisis de riesgos que incluya:

1. determinar qué se trata de proteger;
2. determinar de qué es necesario protegerse;
3. determinar cuan probables son las amenazas;
4. implementar los controles que protejan los bienes informáticos de una manera rentable; y
5. revisar continuamente este proceso y perfeccionarlo cada vez que una debilidad (vulnerabilidad) sea encontrada.

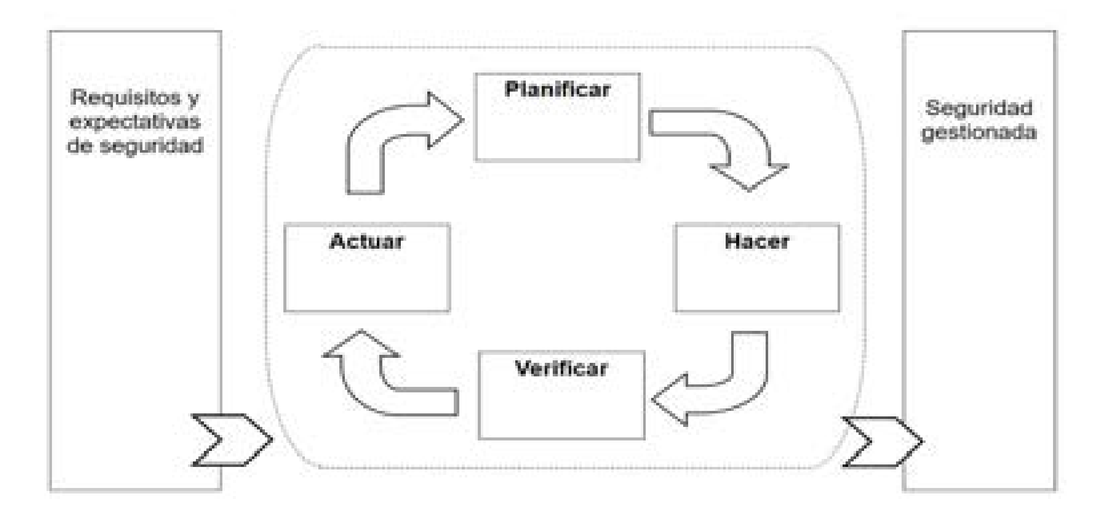
Los tres primeros aspectos son imprescindibles para tomar decisiones efectivas sobre seguridad. Sin un conocimiento razonable de lo que se quiere proteger, contra qué protegerlo y cuan probables son las amenazas, seguir adelante carece de sentido.

La presente metodología promueve la adopción de un enfoque basado en procesos, con el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de una organización; para ello adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI en correspondencia con la NC-ISO-IEC 27001"Requisitos de los Sistema de Gestión de la Seguridad de la Información" y adecuada a la NC-ISO-IEC 17799 (27002) "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".

Primera Parte: Sistema de Gestión de la Seguridad Informática

Procesos de un Sistema de Gestión de la Seguridad Informática

El SGSI se compone de cuatro procesos básicos:



Modelo PHVA aplicado a los procesos del SGSI

Planificar (Establecer el SGSI)	Establecer las políticas, los objetivos, procesos y procedimientos de seguridad necesarios para gestionar el riesgo y mejorar la seguridad informática, con el fin de entregar resultados acordes con las políticas y objetivos globales de la organización.
Hacer (Implementar y operar el SGSI)	Tiene como objetivo fundamental garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.
Verificar (Revisar y dar seguimiento al SGSI)	Evaluar y, en donde sea aplicable, verificar el desempeño de los procesos contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
Actuar (Mantener y mejorar el SGSI)	Emprender acciones correctivas y preventivas basadas en los resultados de la verificación y la revisión por la dirección, para lograr la mejora continua del SGSI.

1. Proceso de Planificación del SGSI

Objetivo principal: La realización del análisis y evaluación de los riesgos de seguridad y la selección de controles adecuados.

En esta primera etapa se crean las condiciones para la realización del diseño, implementación y gestión del Sistema de Seguridad Informática, para lo cual se realiza un estudio de la situación del sistema informático desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutan en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad apropiados para gestionar el riesgo y mejorar la seguridad informática, lo cual posibilita obtener resultados conformes con las políticas y objetivos globales de la organización.

Los bienes informáticos de que dispone una entidad no tienen el mismo valor, e igualmente, no están sometidos a los mismos riesgos, por lo que es imprescindible la realización de un análisis de riesgos que ofrezca una valoración de los bienes informáticos y las amenazas a las que están expuestos, así como una definición de la manera en que se gestionan dichos riesgos para reducirlos.

Como resultado, se establecen las prioridades en las tareas a realizar para minimizar los riesgos, puesto que estos nunca desaparecen totalmente. La dirección de la entidad asume el riesgo residual, o sea, el nivel restante de riesgo después de su tratamiento.

1.1. Preparación

Durante la preparación se crean las condiciones para el diseño e implementación del SGSI, y se consideran los aspectos siguientes:

1. Asegurar el compromiso de la dirección.
2. Seleccionar y preparar a los miembros del equipo que participa en el diseño e implementación del SGSI.
3. Recopilar información de seguridad.

1.1.1. Compromiso de la dirección de la entidad con la Seguridad Informática

La dirección apoya activamente la seguridad dentro de la organización mediante una orientación clara, compromiso demostrado y la asignación explícita de las responsabilidades de seguridad informática y su reconocimiento, para lo cual:

a) Asegura que los objetivos de seguridad informática estén identificados, cumplan los requisitos de la organización y están integrados en los procesos principales;

b) formula, revisa y aprueba las políticas de seguridad informática;

c) revisa la efectividad de la implementación de las políticas de seguridad;

d) provee una orientación clara y apoyo visible hacia las iniciativas de seguridad;

e) proporciona los recursos necesarios para la seguridad;

f) aprueba la asignación de los roles específicos y responsabilidades en seguridad informática en la organización;

g) inicia planes y programas para mantener la concienciación en seguridad; y

h) asegura que la implementación de los controles de seguridad informática sea coordinada en toda la organización.

1.1.2. Seleccionar y preparar a los miembros del equipo que participan en el diseño e implementación del SGSI

El proceso de diseño e implementación del SGSI no se realiza por una sola persona o por un grupo de personas de una misma especialidad, sino que es el resultado de un trabajo multidisciplinario en el que participen todos aquellos que de manera integral puedan garantizar el cumplimiento de los objetivos planteados.

El equipo de diseño e implementación se conforma con:

1. Directivos y funcionarios que, a los diferentes niveles, responden por la información que se procesa en las tecnologías y por tanto son los garantes de su protección.
2. Personal de informática que domina los aspectos técnicos necesarios para la implementación de los controles de seguridad.
3. Profesionales de la protección, a partir de su responsabilidad en la custodia de los bienes informáticos y otros que se consideren de acuerdo con su perfil.

1.1.3. Recopilar información de seguridad

Durante el proceso de preparación se reúne toda la información que facilite el diseño e implementación del SGSI, para lo que se utilizan los documentos normativos y metodológicos que existan sobre el tema; documentación de aplicaciones y sistemas en explotación en la organización; documentación de incidentes ocurridos en la entidad o en otras organizaciones afines; tendencias de seguridad nacionales e internacionales, así como otros materiales que faciliten su realización.

1.2. Determinación de las necesidades de protección

Las necesidades de protección del sistema informático se establecen mediante la realización de un análisis de riesgos, que es el proceso dirigido a determinar la probabilidad de que las amenazas se materialicen sobre los bienes informáticos e implica la identificación de los bienes a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que puedan causar.

La realización del análisis de riesgos proporciona:

a) Una detallada caracterización del sistema informático objeto de protección;
b) la creación de un inventario de bienes informáticos a proteger;
c) la evaluación de los bienes informáticos a proteger en orden de su importancia para la organización;
d) la identificación y evaluación de amenazas y vulnerabilidades;
e) la estimación de la relación importancia-riesgo asociada a cada bien informático (peso de riesgo).

En el proceso de análisis de riesgos se pueden diferenciar dos aspectos:

1. La **Evaluación de Riesgos** orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valoran los riesgos y establecen sus niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la entidad; consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar su importancia.
2. La **Gestión de Riesgos** que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:
   a) Reducir la probabilidad de que una amenaza ocurra;
   b) limitar el impacto de una amenaza, si esta se manifiesta;
   c) reducir o eliminar una vulnerabilidad existente; y
   d) permitir la recuperación del impacto o su transferencia a terceros.

La gestión de riesgos implica la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos en una entidad; implica una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas. Para ello se cuenta con las técnicas de manejo del riesgo siguientes:

1. **Evitar:** Impedir el riesgo con cambios significativos en los procesos por mejoramiento, rediseño o eliminación, y es el resultado de adecuados controles y acciones realizadas.
2. **Reducir:** Cuando el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible; esta opción es la más económica y sencilla y se consigue con la optimización de los procedimientos y con la implementación de controles.
3. **Retener:** Cuando se reduce el impacto de los riesgos pueden aparecer riesgos residuales; dentro de las estrategias de gestión de riesgos de la entidad se plantea como manejarlos para mantenerlos en un nivel mínimo.
4. **Transferir:** Es buscar un respaldo contractual para compartir el riesgo con otras entidades, por ejemplo alojamiento, hospedaje, externalización de servicios, entre otros; esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar este.

La necesidad de la actualización permanente del análisis de riesgos está determinada por las circunstancias siguientes:

a) Los elementos que componen un sistema informático en una entidad están sometidos a constantes variaciones: cambios de personal, nuevos locales, nuevas tecnologías, nuevas aplicaciones, reestructuración de entidades, nuevos servicios y otros;
b) la aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes; y
c) pueden aparecer nuevas vulnerabilidades o variar o incluso desaparecer alguna de las existentes, y originan, modifican o eliminan posibles amenazas.

En resumen, durante la determinación de las necesidades de protección del sistema informático es necesario:

1. Caracterizar el sistema informático.
2. Identificar las amenazas potenciales y estimar los riesgos sobre los bienes informáticos.
3. Evaluar el estado actual de la seguridad.

1.2.1. Caracterización del sistema informático

Para el diseño e implementación de cualquier sistema es imprescindible el conocimiento pleno del objeto sobre el cual se quiere diseñar o implantar. Para ello lo más apropiado es precisar los elementos que permitan identificar sus especificidades.

La caracterización del sistema informático incluye la determinación de los bienes informáticos que requieren ser protegidos, su valoración y clasificación según su importancia.

Se precisan los datos que permitan determinar cómo fluye la información entre los diferentes elementos de la entidad, así como entre la entidad y otras instituciones; se considera el carácter de la información y su nivel de clasificación de acuerdo con lo establecido en el país.

Durante la caracterización del sistema informático es necesario establecer además las características de las edificaciones y locales donde están instalados los equipos, tipo de construcción y estructura, lugares o puntos de acceso (ventanas y puertas), visibilidad desde el exterior, ubicación de las TIC, tipos de tecnologías, software instalado, nivel de clasificación de la información que se procesa, documentación de software, preparación y conocimiento del personal que opera los equipos, cualquier otro aspecto que haga más precisa su descripción.

Una buena caracterización del sistema informático permite conocerlo a plenitud y evita pérdida de tiempo e imprecisiones.

Una posible agrupación por categorías que puede ayudar a la identificación de los bienes informáticos a proteger, podría ser la siguiente:

1. **Hardware:** Redes de diferente tipo, servidores y estaciones de trabajo, computadoras personales (incluyen portátiles), soportes magnéticos, ópticos y removibles, líneas de comunicaciones, módems, ruteadores, concentradores, entre otros.
2. **Software:** Programas fuentes, programas ejecutables, programas de diagnóstico, programas utilitarios, sistemas operativos, programas de comunicaciones, entre otros.
3. **Datos:** Generados durante la ejecución, almacenados en discos, información de respaldo, bases de datos, trazas de auditoría, en tránsito por los medios de comunicaciones, entre otros.
4. **Personas:** Usuarios, operadores, programadores, personal de mantenimiento, entre otros.
5. **Documentación:** De programas, de sistemas, de hardware, de procedimientos de administración, entre otros.

Una vez identificados los bienes informáticos que necesitan ser protegidos, se determina su importancia dentro del sistema informático y se clasifican según esta.

La valoración de los bienes informáticos posibilita mediante su categorización, determinar en qué medida uno es más importante que otro (grado de importancia) y se toman en cuenta aspectos tales como: la función que realizan, su costo, la repercusión que ocasionaría la pérdida y posibilidad de su recuperación; así como la preservación de la confidencialidad, la integridad y la disponibilidad.

Al estimar la repercusión que ocasiona la pérdida de un bien informático se tiene en cuenta el tiempo que la entidad puede seguir el trabajo sin este, lo que puede ser vital para su funcionamiento. Este tiempo puede oscilar entre escasas horas, hasta días y semanas. Por ejemplo: una agencia bancaria no puede prescindir de su Plan de Cuentas por un número considerable de horas, porque sería imposible su funcionamiento.

Se da el caso que un bien informático puede estar hasta tres semanas dañado. Esto depende de su ciclo de utilización, por ejemplo: si la nómina de una entidad se daña días antes del pago a los trabajadores pondría a la entidad en un serio aprieto, si se dañó después del cobro, habría más tiempo para su recuperación.

La determinación de la importancia de cada bien informático puede ser realizada de forma descriptiva (por ejemplo, valor alto, medio, bajo) o de forma numérica asignan valores entre cero y diez (0 si tiene poca importancia y 10 sí es máxima).

Un resultado inmediato de la caracterización del sistema informático es la conformación de un listado que contenga la relación de los bienes informáticos identificados y clasificados según su importancia.

Bienes informáticos críticos

Como resultado de la evaluación anterior se determinan los bienes informáticos críticos para la gestión de la entidad en virtud de la función que realizan o los servicios que proporcionan, su importancia y el riesgo a que están sometidos. Se consideran bienes informáticos críticos aquellos sin los cuales el trabajo de la entidad no tuviera sentido o no puede ser ejecutado. Por ejemplo:

a) El servidor principal de una red;
b) los medios de comunicaciones de un centro de cobros y pagos remoto;
c) el sistema de control de tráfico aéreo de un aeropuerto;
d) el sistema contable de una entidad.

Los bienes informáticos críticos tienen carácter relativo según la entidad de que se trate, por ejemplo: la destrucción o modificación de una base de datos en una escuela secundaria probablemente no tenga la misma connotación que si ocurre en un centro de investigaciones científicas.

Un aspecto de vital importancia es la concatenación, o sea, la dependencia entre un bien informático y otro. En la práctica se da el caso que un bien informático resulta no ser importante tratado individualmente, para el correcto funcionamiento de una tarea cualquiera, pero como elemento de un sistema, es el preámbulo o paso anterior obligado para el funcionamiento de otro bien informático que ha sido marcado como importante. En este caso todos los activos que cumplen con esa condición han de ser considerados como importantes.

Por otra parte, puede que un recurso sea muy costoso y por ello considerado de importancia alta, y sin embargo no es imprescindible para la gestión de la entidad. Estas circunstancias pueden elevar de forma artificial el nivel de importancia con que ha sido catalogado.

El equipo de trabajo controla que las distintas estructuras que conforman la entidad no declaren importantes aquellos bienes informáticos que en realidad no lo son. Esto evitaría gastos innecesarios. Existe la tendencia de declarar como importantes (críticos) a bienes informáticos que en realidad no lo son. A la hora de tratar este aspecto el equipo de trabajo es lo suficientemente paciente y persuasivo para evitar esta perjudicial práctica.

Lo anterior implica un análisis complementario de los datos obtenidos en el listado de bienes informáticos, que se realiza de la forma siguiente:

1. Señale adecuadamente aquellos bienes informáticos que fueron valorados de importancia significativa.
2. Señale aquellos bienes informáticos, que no han sido valorados de importancia significativa, y tienen una incidencia directa con algún otro bien informático crítico.
3. Señale después de un estudio riguroso y detallado, aquellos bienes informáticos que no tienen una valoración significativa, ni incidencia directa en el trabajo de bienes informáticos críticos, y resulta necesario que sean marcados como tales, por razones prácticas.
4. Ordene el listado de bienes informáticos a partir de las consideraciones anteriores.

1.2.2. Identificación de las amenazas sobre el sistema informático

Una vez que los bienes informáticos que requieren protección son identificados y valorados según su importancia, es necesario identificar las amenazas sobre estos y estimar el daño (impacto) que puede producir su materialización.

Para cada bien informático a proteger los objetivos fundamentales de seguridad son la confidencialidad, la integridad y la disponibilidad, por lo que hay que determinar cada amenaza sobre la base de como pueda afectar a estas características de la información. El peso que cada una de estas características tiene para los bienes informáticos varía de una entidad a otra, en dependencia de la naturaleza de los procesos informáticos que se llevan a cabo en función de su objeto social. Algunas de las amenazas más comunes son las siguientes:

a) Pérdida de información;
b) corrupción o modificación de información;

c) sustracción, alteración o pérdida de equipos o componentes;
d) divulgación de información; e
e) interrupción de servicios.

La realización de un análisis de riesgos implica el examen de cada una de las amenazas sobre los bienes informáticos y su clasificación por niveles, a partir de la probabilidad de su ocurrencia y la severidad del impacto que puedan producir.

1.2.3. Estimación del riesgo sobre los bienes informáticos

La estimación del riesgo sobre cada bien informático se determina con la consideración de las probabilidades de materialización de las amenazas que actúan sobre este. Esto puede ser realizado de forma descriptiva (por ejemplo: riesgo alto, medio, bajo) o de forma numérica asignan valores entre cero y uno (0 si la probabilidad de que se materialice la amenaza es nula y 1 si es máxima).

Una amenaza puede incidir sobre varios bienes informáticos con la misma probabilidad y sin embargo sus consecuencias no necesariamente son iguales, dependen en cada caso de la importancia del bien de que se trate. La interrelación entre la probabilidad de materialización de las amenazas que actúan sobre un bien informático y la importancia estimada de este, determinan el peso del riesgo. De esta manera se puede determinar el peso del riesgo para cada bien informático.

La evaluación de los riesgos posibilita conocer que bienes informáticos, o que áreas en particular están sometidas a un mayor peso de riesgo y su naturaleza, lo que permite la selección adecuada de los controles de seguridad que son establecidos en cada uno de los casos, y se garantiza de esta manera una correcta proporcionalidad por medio de una adecuada relación entre costos y beneficios.

Es necesario precisar de una manera exhaustiva los riesgos a que está sometido el sistema en cada una de sus partes componentes, a partir de lo cual se pueden determinar con racionalidad los controles de seguridad que son implementados.

La aplicación de los elementos aquí expuestos puede ser realizada con mayor o menor rigor, en dependencia de la composición y preparación del equipo de trabajo designado para acometer esta tarea y de la participación que se dé a otras personas, que sin formar parte del equipo, puedan brindar los elementos que se requiera.

Por otra parte, desde el momento que los resultados dependen de valores estimados, las conclusiones a que se arribe son tomadas como una aproximación al problema, que puede ser ajustada en sucesivas versiones, en correspondencia con la práctica diaria. Los conceptos anteriormente expresados pueden ser aplicados en diversas variantes, pero de alguna forma es imprescindible utilizarlos.

1.2.4. Evaluación del estado actual de la Seguridad Informática

Generalmente las entidades que emplean las TIC en el desarrollo de su actividad, aunque no hayan diseñado un sistema de seguridad informática que considere de forma integral todos los factores a tener en cuenta, tienen implementadas determinadas normas, medidas y procedimientos de seguridad, generalmente de forma empírica a partir de incidentes que han ocurrido o de las experiencias de otras entidades, lo que es insuficiente y da lugar a la existencia de vulnerabilidades.

Es necesario evaluar de manera crítica la efectividad de los controles existentes, sobre la base de los resultados del análisis de riesgos realizado, con el objetivo de perfeccionarlos o sustituirlos por aquellos que brinden la respuesta adecuada. Los resultados de esta evaluación ayudan a orientar y a determinar una apropiada acción gerencial y las prioridades para gestionar los riesgos de seguridad informática, así como la implementación de los controles seleccionados para protegerse.

La determinación de las necesidades de protección examinada en este apartado da como resultado la definición de los aspectos principales siguientes:

1. Cuáles son los bienes informáticos más importantes a proteger.
2. Qué amenazas tienen mayor probabilidad de actuar sobre los bienes informáticos y su posible impacto sobre la entidad.
3. Qué áreas están sometidos a un mayor peso de riesgo y qué amenazas los motivan.
4. Qué controles de seguridad son perfeccionados o sustituidos y en qué caso se requiere definir e implementar alguno nuevo.

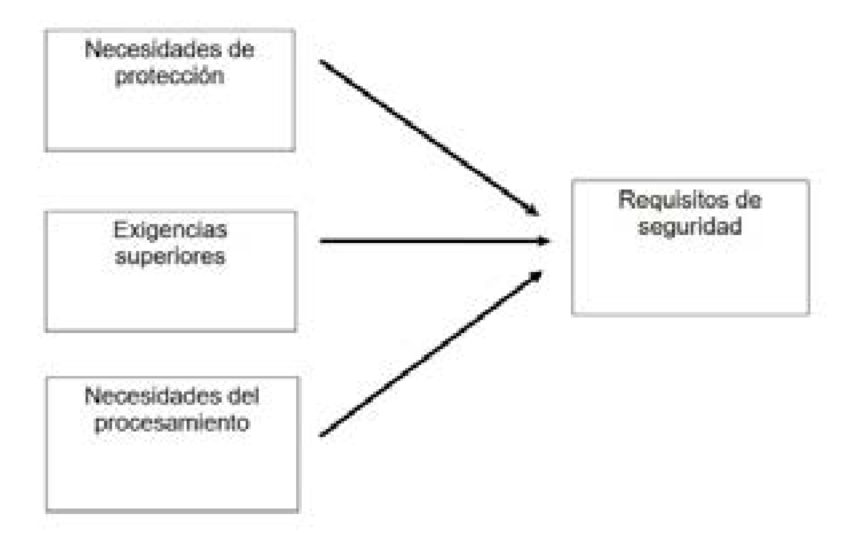
Llegado a este punto es necesario:

1. Identificar y evaluar alternativas posibles para tratar los riesgos.
2. Seleccionar e implantar los controles que permitan reducir el riesgo a un nivel aceptable.
3. Identificar los riesgos residuales que han quedado sin cubrir.
4. Preparar un plan para el tratamiento de los riesgos.
5. Preparar procedimientos para implantar los controles.

1.3. Establecimiento de los requisitos de Seguridad Informática

Parte esencial del proceso de planificación consiste en la identificación de los requisitos de seguridad de la organización. Existen tres fuentes principales:

1. La determinación de las necesidades de protección de la organización, durante la cual se identifican los bienes informáticos más importantes; las amenazas a que están sometidos; se evalúa la vulnerabilidad y la probabilidad de ocurrencia de las amenazas y se estima su posible impacto.
2. El conjunto de requisitos instituidos por obligaciones contractuales, normas legales y técnicas que satisfacen la organización.
3. Los principios, objetivos y requisitos que forman parte del procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.



Los requisitos de seguridad se identifican mediante la evaluación de los riesgos. El gasto en controles se equilibra con el perjuicio para la organización resultante de los fallos de seguridad (costo-beneficio).

1.4. Selección de los controles de Seguridad Informática

Antes de considerar el tratamiento de los riesgos, la organización decide los criterios para determinar si pueden ser aceptados o no. Un riesgo puede ser aceptado si, por ejemplo, se determina que es bajo o que el costo de su tratamiento no es rentable para la organización. Para cada uno de los riesgos identificados se toma una decisión sobre su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) **Aplicar controles apropiados** para reducir los riesgos;
b) **Aceptar riesgos** de manera consciente y objetiva, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos;
c) **Evitar riesgos**, no permitir las acciones que propicien los riesgos;
d) **Transferir los riesgos** a otras partes, por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde se decida aplicar controles apropiados, se seleccionan e implantan para lograr los requisitos identificados mediante la evaluación de riesgos. Los controles aseguran que estos son reducidos a un nivel aceptable y se toman en cuenta:

a) Requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales;
b) objetivos de la organización;
c) requisitos y restricciones operacionales;
d) costo de la implementación y de la operación;
e) la necesidad de balancear la inversión en la implementación y la operación de controles contra el daño probable como resultado de fallas de la seguridad.

Los controles de seguridad que se seleccionen para la reducción de los riesgos a un nivel aceptable cubren adecuadamente las necesidades específicas de la organización. La selección de los controles de seguridad depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, las opciones para su tratamiento, y el acercamiento a su gestión general aplicada a la organización, y también está conforme con toda la legislación y regulaciones nacionales e internacionales vigentes.

Los objetivos de control y los controles se basan en: los resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo; en los requisitos legales o reglamentarios; en las obligaciones contractuales y en las necesidades orgánicas de la entidad en materia de seguridad informática.

Los controles de seguridad informática son considerados en las etapas de especificación de requisitos y de diseño de sistemas y aplicaciones. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y en el peor de los casos, imposibilidad de alcanzar la seguridad adecuada. Estos controles son establecidos, implementados, supervisados y mejorados cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Hay que tener presente que ningún sistema de controles puede alcanzar la seguridad completa y que acciones adicionales de gestión se implementan para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización.

La seguridad informática se logra implantar con un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software. Nos referiremos a continuación específicamente a las políticas y a las medidas y procedimientos de seguridad informática.

1.4.1. Políticas de Seguridad Informática

El objetivo fundamental de la definición de las Políticas de Seguridad Informática consiste en proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos de la organización y con las regulaciones y leyes vigentes.

La dirección establece políticas de seguridad en correspondencia con los objetivos de la entidad y demuestra su apoyo y compromiso a la seguridad informática, con la publicación y el mantenimiento de esas políticas en toda la organización, las cuales se comunican a todos los usuarios de manera apropiada, accesible y comprensible.

Las políticas de seguridad definen los "QUE": **qué** debe ser protegido, **qué** es más importante, **qué** es más prioritario, **qué** está permitido y **qué** no lo está y **qué** tratamiento se le dan a los problemas de seguridad. Las políticas de seguridad en sí mismas no dicen "COMO" las cosas son protegidas. Esto es función de las medidas y procedimientos de seguridad.

Las políticas de seguridad conforman la estrategia general. Las medidas y procedimientos establecen en detalle los pasos requeridos para proteger el sistema informático. No puede haber medidas y procedimientos que no respondan a una política, al igual que no puede concebirse una política que no esté complementada con las medidas y procedimientos que le correspondan.

Comenzar con la definición de las políticas de seguridad a partir de los riesgos estimados asegura que las medidas y procedimientos proporcionen un adecuado nivel de protección para todos los bienes informáticos.

Desde que las políticas de seguridad pueden afectar a todo el personal en una entidad es conveniente asegurar tener el nivel de autoridad requerido para su establecimiento. La creación de las políticas de seguridad es avalada por la máxima dirección de la organización que tiene el poder de hacerlas cumplir. Una política que no se puede implementar y hacer cumplir es inútil.

Uno de los objetivos básicos al desarrollar las políticas de seguridad consiste en definir qué se considera uso apropiado de los sistemas informáticos; así como la forma en que se tratan los incidentes de seguridad. Para esto son considerados los criterios siguientes:

1. Tener en cuenta el objeto social de la entidad y sus características. Por ejemplo la seguridad de una entidad comercial es muy diferente a la de un organismo central o a la de una universidad.
2. Las políticas de seguridad que se desarrollen están en correspondencia con las políticas, reglas, regulaciones y leyes a las que la entidad está sujeta.
3. A menos que el sistema informático a proteger esté completamente aislado e independiente, hay que considerar las implicaciones de seguridad en un contexto más amplio. Las políticas manejan los asuntos derivados de un problema de seguridad que tiene lugar por causa de un sitio remoto, así como un problema que ocurre en este como resultado de un usuario o computadora local.

Algunas de las interrogantes que se resuelven al diseñar una política de seguridad son las siguientes:

1. ¿Qué estrategia se adopta para la gestión de la seguridad informática?
2. ¿A quién se le permite utilizar los bienes informáticos?
3. ¿Qué se entiende por uso correcto de los recursos?
4. ¿Quién está autorizado para garantizar el acceso y aprobar el uso de los bienes informáticos?
5. ¿Quién tiene privilegios de administración de los sistemas?

6. ¿Cuáles son los derechos y responsabilidades de los usuarios?
7. ¿Cuáles son los derechos y responsabilidades de los administradores de sistemas frente a los de los usuarios?
8. ¿Qué hacer con la información clasificada y limitada?
9. ¿Qué hacer ante la ocurrencia de un incidente de seguridad?

Estas no son las únicas interrogantes que son resueltas en el diseño de las políticas. En la práctica surgen otras no menos importantes.

Las principales características que tiene una buena política de seguridad son:

1. Poder implementarse a través de medidas y procedimientos, la publicación de principios de uso aceptable u otros métodos apropiados.
2. Poder hacerse cumplir por medio de herramientas de seguridad, donde sea apropiado y con sanciones, donde su prevención no sea técnicamente posible.
3. Definir claramente las áreas de responsabilidad de los usuarios, administradores y directivos.

Entre los componentes que forman parte de las políticas de seguridad se incluyen:

a) El tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría;

b) el empleo conveniente y seguro de las tecnologías instaladas y cada uno de los servicios que estas pueden ofrecer;

c) la definición de los privilegios y derechos de acceso a los bienes informáticos para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación, mediante la especificación de las facultades y obligaciones de los usuarios, especialistas y directivos;

d) los aspectos relacionados con la conexión a redes de alcance global y la utilización de sus servicios;

e) el establecimiento de los principios que garanticen un efectivo control de acceso a las tecnologías (incluyen el acceso remoto) y a los locales donde estas se encuentren;

f) las normas generales relacionadas con la información de respaldo y su conservación;

g) los principios a tener en cuenta sobre los requerimientos de Seguridad Informática que deben ser considerados en la adquisición de nuevas tecnologías;

h) los aspectos relacionados con la adquisición por cualquier vía de software y documentos de fuentes externas a la entidad y la conducta a seguir en estos casos;

i) la definición de las responsabilidades de los usuarios, especialistas y directivos, sus derechos y obligaciones con respecto a la Seguridad Informática;

j) la definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuario, entre otros;

k) las normas a tener en cuenta en relación con el mantenimiento, reparación y traslado de las tecnologías y del personal técnico (interno y externo) que requiere del acceso a estas por esos motivos;

l) los principios generales para el tratamiento de incidentes y violaciones de seguridad, qué se considera incidente de seguridad y a quién reportar.

Las políticas de seguridad informática son revisadas a intervalos programados o ante el surgimiento de cambios significativos para asegurar su actualización, adecuación y efectividad.

A continuación se muestran dos ejemplos de políticas:

1. El acceso a las áreas o zonas controladas se permite exclusivamente al personal autorizado.

2. El acceso a los medios informáticos es expresamente autorizado por el jefe facultado.

Obsérvese que en el primer ejemplo la política expresada limita explícitamente al personal autorizado el acceso a las áreas o zonas controladas, pero no especifica cuáles son las áreas o zonas definidas como controladas, cómo se garantiza el control en cada una de ellas, qué personal es autorizado, quién está facultado para otorgar las autorizaciones, cuándo se requieren estas autorizaciones y qué forma tiene la autorización (por escrito, verbal, etc.). Es aplicable en todas las áreas controladas de la entidad independientemente de su categoría (limitada, restringida o estratégica) y de la forma de su implementación en cada caso.

De igual manera en el segundo ejemplo, no se menciona cómo se realiza la autorización de los usuarios para acceder a los medios informáticos, cuándo se efectúe, ni quién es la persona facultada para hacerlo.

Todas esas "aparentes insuficiencias" corresponden ser despejadas con medidas y procedimientos ajustados a las características propias de cada lugar donde corresponda aplicar esas políticas, que por supuesto no tienen por qué ser iguales en cada caso. Por ello las medidas y procedimientos sí tienen que especificar en detalle lo que hay que hacer, pues al contrario de las políticas que están destinadas para toda la entidad, son específicas en función de las necesidades de cada área.

De lo anterior se infiere que cualquier política que se establezca necesita ser instrumentada mediante las medidas y procedimientos que garanticen su cumplimiento en cada área que lo necesite y viceversa. Debido a esto, se requiere contrastar las medidas y procedimientos que se implanten con las políticas definidas para comprobar que no existan unas sin respaldo de las otras.

1.4.2. Medidas y procedimientos de Seguridad Informática

Las medidas y procedimientos de seguridad que se implementen en correspondencia con las políticas definidas, conforman el cuerpo del sistema de seguridad diseñado y representan la línea de defensa básica de protección de los bienes informáticos, por lo que es sumamente importante su selección adecuada, de forma tal que cubran las amenazas identificadas durante el proceso de evaluación de riesgos, y se implementen de una manera rentable.

Si la mayor amenaza al sistema es un acceso remoto, tal vez no tenga mucha utilidad el empleo de dispositivos técnicos de control de acceso para usuarios locales. Por otro lado si la mayor amenaza es el uso no autorizado de los bienes informáticos por los usuarios habituales del sistema, probablemente es necesario establecer rigurosos procedimientos de monitoreo y de gestión de auditoría.

Las medidas y procedimientos que se establecen son definidos de manera suficientemente clara y precisa, para evitar interpretaciones ambiguas por parte de los responsabilizados con su cumplimiento.

La seguridad es implementada mediante el establecimiento de múltiples barreras de protección, la selección de controles de diferentes tipos de forma combinada y concéntrica, para lograr con ello una determinada redundancia que garantice que si una medida falla o resulta vulnerada, la siguiente medida entre en acción y continúe la protección del activo o recurso. No es conveniente que el fallo de un solo mecanismo comprometa totalmente la seguridad.

La implementación de múltiples medidas simples puede en muchos casos ser más seguro que el empleo de una medida muy sofisticada. Esto cobra mayor validez cuando determinada medida no puede ser aplicada por alguna limitación existente, como pueden

ser, por ejemplo: las insuficiencias del equipamiento, que impiden la implementación de una medida técnica. En este caso son consideradas medidas o procedimientos complementarios de otro tipo, que garanticen un nivel de seguridad adecuado.

Hay que tener en cuenta también que el uso del sentido común y una buena gestión son las herramientas de seguridad más apropiadas. De nada vale diseñar un sistema de medidas muy complejo y costoso si se pasan por alto los controles más elementales. Por ejemplo, independientemente de cuán sofisticado sea un sistema de control de acceso, un simple usuario con una clave pobre o descuidada puede abrir las puertas del sistema.

Otro elemento importante a considerar al implementar las medidas y procedimientos es aplicar el principio de proporcionalidad o racionalidad, que consiste en ajustar su magnitud al riesgo presente en cada caso. Por ejemplo, la salva de la información puede tener diferentes requerimientos en distintas áreas y en una misma área para distintos tipos de datos o programas.

Las medidas de Seguridad Informática se clasifican de acuerdo con su origen en: administrativas; de seguridad física, técnica o lógica; de seguridad de operaciones; legales y educativas. A su vez, por su forma de actuar, las medidas pueden ser: preventivas, de detección y de recuperación.

Medidas administrativas

Las medidas administrativas, frecuentemente no son apreciadas en toda su importancia, a pesar de que la práctica ha demostrado que un elevado por ciento de los problemas de seguridad se puede evitar con medidas de esta naturaleza.

Se establecen por la dirección de cada entidad mediante las regulaciones comprendidas dentro de sus facultades y por tanto, son de obligatorio cumplimiento por todo el personal hacia el cual están dirigidas.

Medidas de seguridad física

Constituyen la primera barrera de protección en un Sistema de Seguridad Informática e introducen un retardo que incrementa el tiempo de materialización de un acto doloso o accidental.

Se aplican a los locales donde se encuentran las tecnologías de información y directamente a estas mismas tecnologías e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

Medidas técnicas o lógicas

Son las de mayor peso dentro de un sistema de Seguridad Informática. Pueden ser implementadas por software, a nivel de sistemas operativos y de aplicaciones o por hardware. El uso combinado de técnicas de software y hardware aumenta la calidad y efectividad en la implementación de este tipo de medidas.

Algunos tipos de medidas técnicas son empleadas para identificar y autentificar usuarios, protección criptográfica, protección contra virus y otros programas dañinos y registro de auditoría, entre otros.

Medidas de seguridad de operaciones

Están dirigidas a lograr una eficiente gestión de la seguridad mediante la ejecución de procedimientos definidos y garantizan el cumplimiento de las regulaciones establecidas por cada entidad y por las instancias superiores a esta.

Medidas legales

Representan un importante mecanismo de disuasión que contribuye a prevenir incidentes de seguridad y sancionar adecuadamente a los violadores de las políticas establecidas por la entidad.

Se establecen mediante disposiciones jurídicas y administrativas, en las que se plasman: deberes, derechos, funciones, atribuciones y obligaciones, así como se tipifican las violaciones y tipos de responsabilidad administrativas, civiles, penales u otras.

Medidas educativas

Están dirigidas a inculcar una forma mental de actuar, mediante la cual el individuo esté consciente de la existencia de un Sistema de Gestión de la Seguridad Informática en el que le corresponde una forma de actuar. Se sustentan en dos elementos fundamentales:

1. La existencia de un Sistema de Gestión de la Seguridad Informática.
2. La participación consciente del hombre en el éxito de los objetivos de seguridad planteados.

Medidas de recuperación

Están dirigidas a garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante cualquier eventualidad que pueda ocurrir, que afecte o ponga en peligro su normal desarrollo.

Se establecen a partir de la identificación de los posibles incidentes o fallas que puedan causar la interrupción o afectación de los procesos informáticos y garantizan las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios para ello.

Procedimientos de Seguridad Informática

La implementación de las políticas de seguridad informática requiere generalmente la realización de un conjunto de acciones para garantizar su cumplimiento. La descripción de esta secuencia de acciones constituye un procedimiento de seguridad. Los procedimientos, al igual que las medidas, se clasifican en procedimientos de prevención, de detección y de recuperación.

Los **procedimientos de prevención** tienen el objetivo de asegurar las acciones que se requieren para evitar que una amenaza se materialice y los **de detección** se dirigen a identificar cualquier tipo de indicio que revele la posible materialización de una amenaza, una amenaza en desarrollo o una vulnerabilidad en los sistemas.

La función de los **procedimientos de recuperación**, por el contrario, no es la de prevenir ni la de detectar la materialización de determinadas amenazas, sino la de establecer las acciones que se ejecutan cuando una amenaza ya se ha materializado y afectan parcial o totalmente los bienes informáticos.

En el desarrollo de los procedimientos se usa un lenguaje preciso y una cuidadosa redacción y quedan claras las ideas principales, de forma tal que resulten comprensibles a quienes corresponda su aplicación. Los procedimientos son autosuficientes.

La importancia del establecimiento de procedimientos correctamente definidos garantiza, además de la uniformidad en la aplicación de las políticas, la seguridad de su cumplimiento y su sistematicidad. Algunos procedimientos de seguridad que pueden ser implementados son:

a) De administración de cuentas de usuarios;
b) de asignación y cancelación de permisos de acceso a las tecnologías y sus servicios;
c) de asignación y cancelación de derechos y privilegios;
d) de gestión de incidentes;
e) de gestión de contraseñas;
f) de gestión de salvas;
g) de realización de auditorías;
h) de acceso a las áreas;
i) de entrada y salida de las tecnologías y sus soportes.

Ejemplo de una política y de algunas medidas y procedimientos para su implementación.

Política: "La información es salvada en soportes magnéticos u ópticos con la periodicidad requerida en cada caso, a fin de garantizar su restablecimiento en caso de incidentes de seguridad".

Medidas:

1. La información que se comparte en los servidores de la red se salva en los casetes de cinta habilitados al efecto, diariamente en dos versiones.
2. Las bases de datos de contabilidad son salvadas en discos reescribibles en dos versiones. Diariamente se salvan las modificaciones realizadas y mensualmente toda la información.

Procedimientos:

a) En los servidores:

1. Realizar la salva de la información que se comparte en los servidores en dos casetes numerados, se alternan diariamente, una hora antes de concluir la jornada de trabajo. Utilizar el casete marcado con el No. 1 los días impares y con el No. 2 los días pares.
   Responsable: Administrador de la red
2. Anotar en el modelo de registro establecido (anexo N) la fecha, la hora y el casete utilizado.
   Responsable: Administrador de la red
3. Verificar integridad de la información salvada.
   Responsable: Jefe de Departamento de Redes
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Redes.
   Responsable: Jefe del Departamento de Redes

b) En el Departamento de Contabilidad:

1. Realizar la salva de las bases de datos en discos compactos, se alternan diariamente, al finalizar la jornada de trabajo y el último día hábil de cada mes. Los discos para la salva diaria están marcados con una franja, se utilizan los de la franja roja para los días impares y los de la franja azul para los días pares. Los discos para la salva mensual son numerados del 1 al 12 en correspondencia con cada mes.
   Responsable: Administrador de la aplicación
2. Anotar en el modelo de registro establecido (anexo M) la fecha, la hora y el disco utilizado.
   Responsable: Administrador de la aplicación
3. Verificar integridad de la información salvada.
   Responsable: Jefe de Departamento de Contabilidad
4. Guardar la salva bajo llave en el archivo metálico ubicado en la oficina del Jefe del Departamento de Contabilidad.
   Responsable: Jefe del Departamento de Contabilidad

1.5. Organización de la Seguridad Informática

Con el objetivo de gestionar la seguridad informática se establece un marco apropiado para iniciar y controlar su implementación dentro de la organización.

1.5.1. Organización interna

La dirección aprueba las políticas de seguridad informática de la entidad, asigna roles de seguridad, coordina y revisa la implementación de la seguridad a través de la organización. Si es necesario, gestiona una fuente de asesoramiento especializada en seguridad

informática. Son establecidos contactos con especialistas de seguridad o grupos externos a la organización, incluyen autoridades pertinentes, para mantenerse al día con tendencias de la industria, seguimiento de normas, métodos de evaluación y proveer puntos de enlace adecuados cuando se deban manejar incidentes de seguridad informática. Se propicia un enfoque multidisciplinario hacia la seguridad informática.

1.5.2. Coordinación de la Seguridad Informática

Las actividades referentes a la seguridad informática son coordinadas por los Consejos de Dirección de los órganos, organismos y entidades, que pueden incluir personal de diferentes partes de la organización con funciones y roles específicos. Esta coordinación:

a) Asegura que las actividades referentes a la seguridad son ejecutadas de acuerdo a las políticas establecidas;
b) identifica cómo manejar los incumplimientos;
c) aprueba metodologías y procedimientos para la seguridad informática, por ejemplo, de evaluación de riesgos, respaldo de la información y tratamiento de incidentes;
d) identifica cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas;
e) evalúa la adecuación y coordinación de la implementación de los controles de seguridad informática;
f) promueve en forma efectiva la educación, la formación y la concienciación en seguridad informática a través de la organización;
g) evalúa la información resultante del tratamiento y análisis de los incidentes de seguridad informática y las acciones recomendadas en su respuesta.

1.5.3. Asignación de responsabilidades sobre Seguridad Informática

Se definen las responsabilidades de seguridad informática del personal vinculado con el sistema informático de acuerdo con su participación en este. La asignación de las responsabilidades de seguridad informática se hace en correspondencia con las políticas de seguridad informática, se definen claramente las responsabilidades asociadas con la protección de los bienes informáticos y para la ejecución de procesos específicos de seguridad, como por ejemplo, la gestión de incidentes. Estas responsabilidades son complementadas, de ser necesario, con medidas y procedimientos específicos.

Las personas con responsabilidades de seguridad asignadas pueden delegar tareas de seguridad a otras, sin embargo, mantienen la responsabilidad y garantizan que cualquier tarea delegada se ha cumplido correctamente. Se establecen claramente las áreas de las cuales los individuos son responsables. En particular se considera lo siguiente:

a) definir y documentar los niveles de autorización;
b) identificar y definir los bienes informáticos y los procesos de seguridad asociados con cada sistema específico;
c) asignar el responsable de cada bien informático o proceso de seguridad y documentar los detalles de dicha responsabilidad.

Se asegura que cada cual conozca su responsabilidad en relación con el mantenimiento de la seguridad y que cada clase de problema tenga alguien asignado para tratarlo; y se involucra a todo el personal relacionado con los bienes informáticos. Por ejemplo, los usuarios son responsables del uso adecuado de sus identificadores y contraseñas y los administradores de redes y sistemas están obligados a cubrir las brechas de seguridad y corregir los errores. Para alcanzar una seguridad efectiva es conveniente lograr una participación lo más amplia posible de todo el personal (o al menos la ausencia de una oposición activa).

Se establecen niveles de responsabilidad asociados con las políticas de seguridad. Por ejemplo, en una red se puede definir un nivel con sus usuarios, donde cada uno tiene la responsabilidad de proteger su cuenta. Un usuario que permita que su cuenta sea comprometida incrementa la posibilidad de comprometer otras cuentas o recursos. Los administradores de redes y sistemas forman otro nivel de responsabilidad; se implementan los mecanismos de seguridad que se requieran.

Queda claro que los usuarios son individualmente responsables de la comprensión y aplicación de las políticas de seguridad de los sistemas que ellos emplean y del uso apropiado de los recursos que les han sido asignados.

1.6. Elaboración del Plan de Seguridad Informática

Una vez cumplidas las actividades anteriores, el siguiente paso es la elaboración del Plan de Seguridad Informática, en lo adelante PSI como constancia documentada del Sistema de Seguridad Informática diseñado y constituye el documento básico que recoge claramente las responsabilidades de cada uno de los participantes en el proceso informático y establece los controles que permiten prevenir, detectar y responder a las amenazas que gravitan sobre el sistema informático de cada entidad.

El objetivo del PSI es establecer los requisitos de seguridad del sistema y en él se especifican los controles previstos en cada área o lugar para cumplirlos. El PSI también describe las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema y refleja las contribuciones de los distintos actores con responsabilidades sobre el SGSI.

En el PSI se refiere **cómo** se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios**.**

Se particularizan en el PSI los controles de seguridad implementados en correspondencia con su naturaleza, de acuerdo con el empleo que se haga de los recursos humanos, de los medios técnicos o de las medidas y procedimientos que cumple el personal. **En la Segunda Parte: Estructura y contenido del Plan de Seguridad Informática** se refieren con mayor detalle los elementos necesarios para la elaboración del PSI.

2. Proceso de Implementación del SGSI

Objetivo principal: garantizar una adecuada implementación de los controles seleccionados y su correcta aplicación.

Durante el proceso de implementación del SGSI se comienzan a gestionar los riesgos identificados mediante la aplicación de los controles seleccionados y las acciones apropiadas por parte del personal definido (recursos humanos), los recursos técnicos disponibles en función de la seguridad (medios técnicos) y las medidas administrativas, que garanticen la implantación de controles efectivos para lograr el nivel de seguridad necesario, en correspondencia con los objetivos de la organización, de manera que se mantenga siempre el riesgo por debajo del nivel asumido por la propia entidad.

Se garantiza que el personal al que se asignen responsabilidades definidas en el SGSI esté en capacidad de realizar las tareas exigidas, mediante la formación y el entrenamiento que les permita adquirir el conocimiento y las habilidades que requieran, en correspondencia con su papel dentro del sistema, para lo que se implementan programas de capacitación.

La organización también asegura que el personal tiene conciencia de la necesidad e importancia de las actividades de seguridad informática que le corresponde realizar y cómo ellas contribuyen al logro de los objetivos del SGSI.

Las actividades de formación y sensibilización incluyen:

1. Concienciar al personal de la importancia que el SGSI tiene para la organización.
2. Garantizar la divulgación, el conocimiento y comprensión de las políticas de seguridad que se implementan.
3. Capacitar a los usuarios en las medidas y procedimientos que se van a implantar.
4. Lograr que el personal esté consciente de los roles a cumplir dentro del SGSI.

Se requiere además precisar el procedimiento de medición de la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a emplear estas mediciones, con la finalidad de evaluar su eficacia para producir resultados comparables y reproducibles y de esta forma, determinar si las actividades de seguridad implementadas satisfacen las expectativas concebidas.

Finalmente se implementan los procedimientos y controles que se requieran para detectar y dar respuesta oportuna a los incidentes de seguridad que se presenten, que incluyen su reporte a las instancias pertinentes.

El proceso de implementación es una etapa crucial del SGSI y tal vez la más difícil. De nada vale haber realizado una buena determinación de las necesidades de protección e incluso haber hecho una excelente selección de los controles de seguridad a aplicar, si no se logra implantarlos en cada lugar, se ajustan a las particularidades de los bienes a proteger y a las exigencias específicas de cada área.

Se puede haber definido, por ejemplo, una refinada política de respaldo de la información en previsión de cualquier tipo de contingencia que pudiera presentarse, y no implementar los procedimientos que determinen con exactitud qué información es preservada; con qué frecuencia se salva, en qué soporte y en cuántas copias; quiénes están encargados de ejecutar esas acciones y cómo se garantiza su protección y conservación, de manera que exista la certeza de su integridad cuando requieran ser utilizadas.

Puede haberse confeccionado un Plan de Seguridad Informática que cumpla a cabalidad los requisitos metodológicos, pero en sus partes esenciales se queda “en el papel” y no se conoce ni se aplica por los que tienen que instrumentar los controles que fueron definidos. Por ejemplo, en ocasiones se especifica en el plan la estructura y fortaleza de las contraseñas de acceso a la red y sin embargo, no se configuran en el servidor las reglas que en correspondencia con lo establecido obliguen a los usuarios a su cumplimiento.

De igual forma, pueden haberse concebido los procedimientos para otorgar o cancelar el acceso a sistemas y servicios pero estos no se conocen o se incumplen por los que tienen que ejecutarlos regularmente. Ejemplos semejantes pueden referirse en relación con la gestión de parches de seguridad, la seguridad de las redes inalámbricas, el control de los soportes removibles, la gestión de incidentes y el análisis y conservación de los registros generados por los sistemas y servicios, por solo citar algunos de los más comunes.

De modo que el proceso de implementación del SGSI para que sea exitoso garantiza la implantación de todos los controles que fueron concebidos y su conocimiento y comprensión por los encargados de ejecutarlos y cumplirlos.

2.1. Programa de Desarrollo de la Seguridad Informática

Puede ser que la implementación de algunos controles requiera de un tiempo adicional, ya sea porque necesitan algún tipo de recursos con que no se cuenta, la realización de gestiones complementarias u otras causas. Las acciones que sean necesarias para lograr la implementación de estos controles se incluyen en un programa que señala los plazos para su cumplimiento y el personal responsabilizado con su ejecución. Los aseguramientos que se deriven de estas acciones son considerados dentro del Plan de Inversiones de la

entidad cuando se requiera. El cumplimiento de este programa contribuye al proceso de mejora continua del SGSI y es actualizado según se ejecute. Algunos aspectos a considerar al elaborar el Programa de Desarrollo de la Seguridad Informática pudieran ser los siguientes:

1. La implementación a mediano y largo plazo de aquellos aspectos que así lo exijan para alcanzar un mayor nivel de seguridad, como por ejemplo la introducción de medios técnicos de seguridad, modificación de locales, etc.
2. La preparación y capacitación del personal en materia de seguridad informática, según su participación en el sistema diseñado, ya sea a través de cursos específicos, mediante la impartición de materias relacionadas con el tema y con acciones de divulgación.
3. La organización y ejecución de controles, inspecciones y auditorías (internas y externas), mencionan con qué frecuencia se realizan, quiénes participan y su contenido.

2.2 Factores Críticos de éxito

La implementación exitosa de los controles seleccionados y su correcta aplicación en una organización presupone, además, la consideración de los factores siguientes:

a) La política de seguridad, objetivos y actividades que reflejen los intereses de la organización;
b) el enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) el apoyo visible y el compromiso de la alta dirección;
d) la buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) la comunicación eficaz de la necesidad de la seguridad a todos los directivos y trabajadores;
f) la distribución a todos los trabajadores de directrices y normas sobre la política de seguridad informática de la organización;
g) suministrar recursos para las actividades de gestión de la seguridad informática;
h) proporcionar concienciación, formación y educación apropiadas;
i) proceso efectivo de gestión de incidentes de seguridad informática;
j) implementación de un sistema de medición para evaluar el desempeño en la gestión de seguridad informática y las sugerencias de mejoras.

Durante el proceso de implementación del SGSI es necesario precisar la aplicación de cada uno de los controles seleccionados en las áreas que los requieren y que cubran los riesgos que para ellas fueron identificados. En este sentido, la participación de los jefes de áreas es determinante, pues corresponde a ellos refrendar que los controles que se establezcan dan plena respuesta a los requerimientos de protección de cada área en particular.

Para cumplir con lo expresado en el párrafo anterior se elabora un cronograma de implementación por áreas, mediante el cual los jefes de estas garanticen:

1. La concienciación del personal sobre la necesidad e importancia de sus actividades de Seguridad Informática y cómo ellas contribuyen al logro de los objetivos del SGSI.
2. La preparación del personal para el cumplimiento de sus obligaciones en cuanto a la Seguridad Informática.
3. La implantación de los controles de seguridad, tanto los comunes para toda la entidad como los específicos para el área.
4. La verificación de que los controles aplicados garantizan el cumplimiento de las políticas de seguridad establecidas en la organización.

5. La precisión de los métodos de evaluación de la eficacia de los controles que se implementen.
6. La identificación de los controles que no es posible implantar y deban ser incluidos en el Programa de Desarrollo de la Seguridad Informática.

No se puede dar por terminado el proceso de implementación del SGSI por el dirigente máximo de la entidad, hasta que en todas las áreas sus jefes acrediten el cumplimiento de estos requisitos.

3. Proceso de Verificación del SGSI

Objetivo principal: Revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

Uno de los aspectos más importantes en el proceso de diseño e implementación de un SGSI es el establecimiento de los indicadores y métricas de gestión. Esto permite a la Dirección valorar si los esfuerzos realizados cumplen o no con los objetivos planteados. Para ello se utiliza la medición como instrumento de control. Es necesario lograr diagnosticar correctamente qué pasa y qué es necesario corregir para poder gestionar.

Mediante el proceso de revisión se comprueba la conformidad con los patrones establecidos y como parte de ello se mide el rendimiento y la eficacia del SGSI, para lo cual se precisa considerar las acciones siguientes:

1. Revisiones periódicas de los indicadores seleccionados.
2. Revisiones de los riesgos residuales y riesgos aceptables.
3. Realización de auditorías internas/externas del SGSI.
4. Comunicación de los resultados de las auditorías a las partes interesadas.

La ejecución de procedimientos de revisión mediante instrumentos de medición posibilita detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios en relación a qué aspectos se controlan y miden para lograr el cumplimiento de las metas planteadas.

Los objetivos de estos procedimientos de revisión son:

1. Evaluar la efectividad de la implementación de los controles de seguridad.
2. Evaluar la eficiencia del SGSI, incluyen mejoras continuas.
3. Proveer estados de seguridad que guíen las revisiones del SGSI, faciliten mejoras a la seguridad y nuevas entradas para auditar.
4. Comunicar valores de seguridad a la organización.
5. Servir como entradas al análisis y tratamiento de riesgos.

La gestión del Sistema de Seguridad Informática se basa en un ciclo de mejora continua, por lo que es vital medir para poder observar cómo las cosas mejoran a medida que el sistema madura. Si no se mide, se trabaja en base a sensaciones, y las decisiones tomadas sin la información necesaria pueden conducir a equivocaciones.

Pasado el tiempo previsto de antemano, hay que volver a recopilar datos de control y analizarlos, compararlos con los objetivos y especificaciones iniciales, para evaluar si se han producido cambios que afecten los resultados esperados. Donde sea aplicable, se mide el desempeño del SGSI contra las políticas y los objetivos de seguridad y la experiencia práctica, y se reporta los resultados a la Dirección, para su revisión.

3.1. Métodos de Medición

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicarse a múltiples aspectos. Por su naturaleza, los métodos de medición pueden ser subjetivos u objetivos. Los métodos subjetivos implican el criterio humano, mientras que los objetivos se basan en una regla numérica, que puede ser aplicada por personas o recursos automatizados. Algunos ejemplos de métodos de medición son:

1. Encuestas/indagaciones.
2. Observación.
3. Entrevistas.
4. Cuestionarios.
5. Evaluación de conocimientos.
6. Inspecciones.
7. Consulta a sistemas.
8. Supervisión.
9. Muestreo.

Para la implementación de estos métodos en cualquier entidad hay disponibles diferentes procedimientos y herramientas que facilitan esta tarea, entre ellas:

1. Utilización de listas de verificación de la conformidad del SGSI con aspectos normados que requieren cumplirse.
2. La aplicación de programas diseñados con este objetivo, como por ejemplo el sistema de evaluación Diógenes elaborado por la Oficina de Seguridad para las Redes Informáticas.
3. La realización de diagnósticos de seguridad presenciales y remotos por especialistas de la propia organización o contratados a terceros.
4. La evaluación de los resultados obtenidos del análisis de los registros de auditoría generados por sistemas y servicios.
5. El análisis de los resultados de la supervisión del empleo de los sistemas y servicios por parte de los usuarios autorizados para ello.
6. Los reportes y alarmas generados por los sistemas de seguridad, como por ejemplo un Sistema de Detección de Intrusos (IDS por sus siglas en inglés).
7. El análisis de los incidentes de seguridad ocurridos a partir de la información registrada sobre estos.
8. El análisis de los reportes de las violaciones de los controles de seguridad.
9. El análisis de las no conformidades detectadas en controles realizados y su erradicación.

La medición sirve para cuestionar continuamente en base a datos y registros, si los controles de seguridad funcionan bien. Se establece un conjunto de indicadores que sirven para evidenciar que lo implementado funciona correctamente.

3.2. Indicadores de medición

En esta etapa adquieren especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del SGSI.

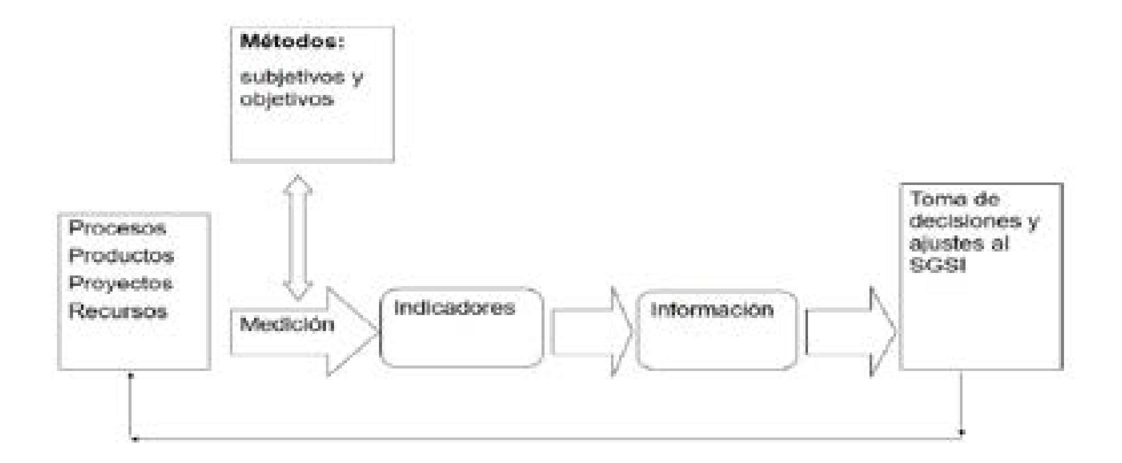
Cada indicador tiene asociado valores que representen las metas a cumplir. En este sentido, cada organización define su criterio respecto a qué aspectos quiere controlar y medir para lograr el cumplimiento de los objetivos. Para ello se pueden definir distintos grupos de indicadores que recojan los diferentes ámbitos que se quieren gestionar. Por tanto, se podrían tener:

1. **Indicadores del grado de efectividad de los controles de seguridad:** Su sentido es valorar si los controles implantados funcionan bien o es necesario ajustarlos.
2. **Indicadores de medición del entorno y la hostilidad:** Su misión es detectar cambios en el entorno y contexto que rodea al SGSI para realizar ajustes respecto al análisis de riesgos por aparición de nuevas amenazas o cambios en sus frecuencias de ocurrencia. Por ejemplo, la aparición de nuevas amenazas internas, cambios en el clima laboral de la organización, frecuencia de publicación de vulnerabilidades, detección de nuevas aplicaciones malware.

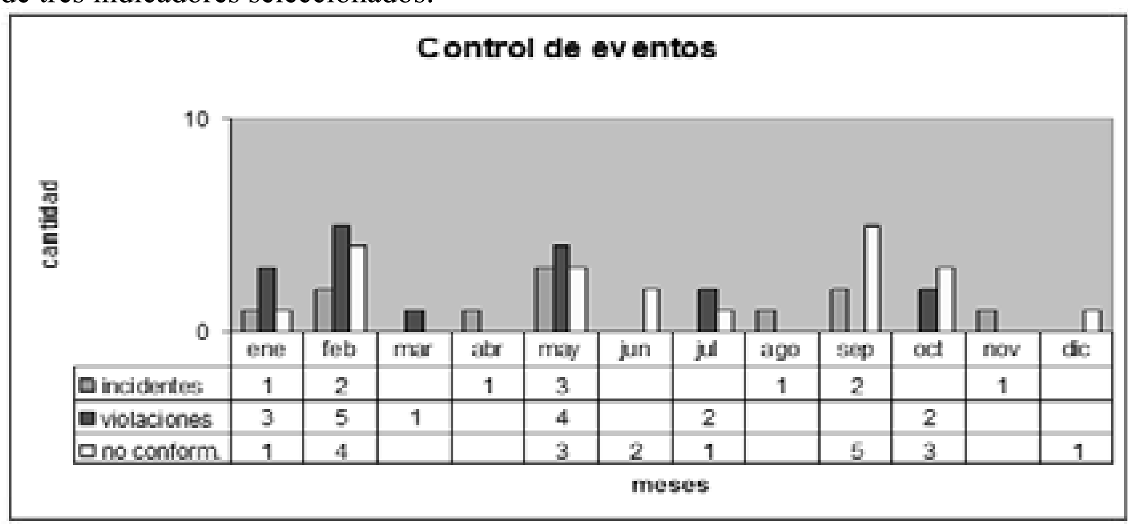
3. **Indicadores de gestión interna:** Estos se establecen para evaluar el funcionamiento propio del propio SGSI y tiene que ver con la monitorización de las tareas propias de gestión. Por ejemplo, las relacionadas con la eliminación en plazo de no conformidades, el porcentaje de cumplimiento de los objetivos planteados, el número de no conformidades detectadas por auditoría.

Al definir y valorar el comportamiento de los indicadores, se tiene muy en cuenta el daño derivado de la ocurrencia de un incidente y su posible impacto en los objetivos de la organización.

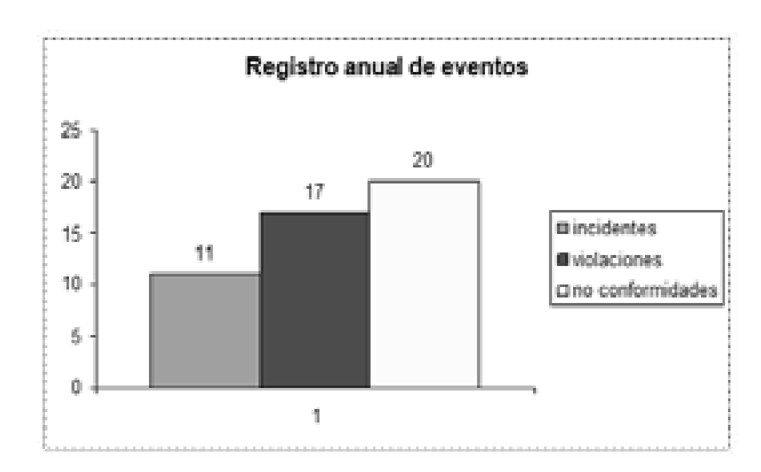
La información referente a estos indicadores, desde la perspectiva de la gestión, es la más crítica, dado que es la base de la retroalimentación del sistema. Por tanto, hay que disponer de sensores de diferente naturaleza y con diferentes objetivos: medir la evolución de la ejecución del plan, valorar el rendimiento y funcionamiento de las medidas de seguridad, vigilar el entorno por si se vuelve más hostil y otros.



Al final lo importante es no perder el sentido del por qué se hacen las cosas. Para ello, toda esta información se transforma en unas sencillas gráficas que la Dirección pueda entender y que sirvan como el auténtico "termómetro de la situación". Estos datos, adecuadamente procesados y visualmente representados, sin disponer de excesivos detalles y conocimientos técnicos, permiten a la Dirección realizar su principal labor dentro del SGSI: tomar decisiones y realizar los ajustes necesarios para el logro de los objetivos. A modo de ejemplo se muestra a continuación una tabla y un gráfico con datos de tres indicadores seleccionados:



	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
incidentes	1	2		1	3			1	2		1	
violaciones	3	5	1		4		2			2		
no conform.	1	4			3	2	1		5	3		1



Otro aspecto a tener en cuenta es el de la frecuencia. Se definen y programan claramente los intervalos en los cuales se lleva a cabo cada medición (semanal, mensual, trimestral, anual y otros), se considera una relación entre la necesidad de contar con esta información y el esfuerzo para obtenerla (costo/beneficio).

Se puede definir un total de factores a evaluar (que nombraremos como K) y ver cuántos de ellos se cumplen (que nombraremos como k).

Por ejemplo: De 10 factores predeterminados se cumplen 7

K = 10 y k = 7

7/10 = 0.7 => 70 %

Algunas posibles relaciones para indicadores pudieran ser:

a) Tiempo sin interrupciones/Tiempo total de servicio;
b) tiempo sin violaciones reportadas/Tiempo total de servicio;
c) 1/cantidad de incidentes computacionales;
d) velocidad real/velocidad contratada;
e) no conformidades detectadas/total de aspectos verificados.

3.3. Reglas que cumple una buena métrica:

1. **Ser objetivas:** Aportan un criterio de recogida de datos medible y objetivo, que no dependa de valoraciones subjetivas.
2. **Ser fáciles de obtener:** Los datos sencillos, simples de calcular y poco costosos de recoger son buenos candidatos a ser métricas. Al respecto, lo más sencillo es recurrir a datos proporcionados por herramientas o procesados de forma automatizada.
3. **Expresables de forma numérica o porcentual**. No se basan en etiquetas cualitativas tales como “alto”, “medio” o “bajo”.
4. **Expresable con el uso de algún tipo de unidad de medida:** Siempre están vinculadas a algo tangible basado en escalas como el tiempo, número de defectos, o cuantías económicas.
5. **Significativas:** Toda buena métrica es significativa, es relevante para el hecho o circunstancia que se desea medir y aporta criterio. Una métrica que no aporta información no es una buena métrica y es desechada.

4. Proceso de Actualización del SGSI

Mantenimiento, mejora y corrección del SGSI

Objetivo principal: Realizar los cambios que sean necesarios para mantener el máximo rendimiento del SGSI

El proceso de actualización del SGSI comprende la aplicación de acciones correctivas y preventivas, basadas en los resultados del proceso de verificación descrito en el apartado anterior, para lograr la mejora continua.

En esta etapa se llevan a cabo las labores de mantenimiento del sistema, así como las acciones de mejora y de corrección identificadas si, tras la verificación, se ha detectado algún punto débil. Este proceso se suele llevar en paralelo con la verificación y se actúa al detectarse la deficiencia, no se espera a tener la fase de verificación completada para comenzar con las tareas de mejora y corrección.

El SGSI se mantiene eficiente durante todo el tiempo y se adapta a los cambios internos de la organización, así como los externos del entorno. Para lograr el perfeccionamiento constante del SGSI se aplican las lecciones aprendidas de las experiencias de seguridad de otras organizaciones, las de la propia entidad y la de los incidentes ocurridos.

Durante la Implementación de los resultados derivados de la verificación se requiere, generalmente, modificar controles e implantar las mejoras identificadas en las revisiones del SGSI a partir de las decisiones sobre los cambios requeridos para mejorar el proceso y en consecuencia se:

1. Estandarizan los cambios de procesos.
2. Comunican los cambios a todos los implicados.
3. Proporciona entrenamiento al personal sobre los nuevos métodos.
4. Evalúan los nuevos riesgos.
5. Modifica el SGSI.
6. Actualiza el PSI.

Se comunican las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, se precisa sobre cómo proceder ante el nuevo escenario y se entrena al personal con el fin de asegurar que las mejoras logren los objetivos previstos.

Algunos ejemplos de circunstancias que implican la necesidad de un nuevo análisis de riesgos pudieran ser las siguientes:

1. Instalación de nuevos tipos de redes (por ejemplo una red inalámbrica) en áreas de la entidad o de algún nuevo enlace para la comunicación con otras instancias.
2. Cambios en la topología de las redes o en la arquitectura de seguridad.
3. Introducción de tecnologías que no se habían empleado con anterioridad.
4. Incremento del empleo de soportes removibles como portadores de información por parte del personal.
5. Ocurrencia de algún incidente de seguridad.
6. Puesta en marcha de una nueva aplicación o introducción de un nuevo servicio de red.
7. Nuevos requerimientos informativos para la organización.
8. Incorporación de personal con poca experiencia y conocimientos.
9. Cambios en la plantilla de personal, en su composición o completamiento.
10. Conversión de locales de uso interno en áreas de acceso público.
11. Modificaciones estructurales de los inmuebles o cambios en su distribución.

Una vez realizados los cambios necesarios para mantener el máximo rendimiento del SGSI, se actualiza el PSI en las partes que corresponda e informan de ello a todos los que requieran conocerlo.

Segunda Parte: Estructura y contenido del Plan de Seguridad Informática

Consideraciones Generales

Para la elaboración del Plan de Seguridad Informática se tienen en cuenta las consideraciones siguientes:

1. El PSI es un documento de trabajo y como tal es accesible a todo el personal que requiera su utilización, por lo que la información que en él se incluye es ordinaria. No se incluye en este, información limitada o clasificada, la cual, de ser necesario, forma parte de un documento independiente que es categorizado conforme con lo establecido en la legislación vigente en materia de seguridad y protección de la información oficial.
2. El PSI se ajusta en todo momento al sistema de seguridad diseñado e implementado, se evitan formalismos y definiciones conceptuales y se utilizan como una herramienta de trabajo para la gestión de la seguridad.
3. Su redacción es simple, clara y libre de ambigüedades para que sea comprensible por todos los involucrados en su cumplimiento.
4. Tiene un carácter impositivo por lo que se evitan términos tales como "se recomienda", "se debe" y otros similares que no implican obligatoriedad.
5. Contiene las tablas, gráficos y otros complementos que contribuyan a su mejor interpretación.
6. Se mantiene permanentemente actualizado sobre la base de los cambios que se produzcan en las condiciones consideradas durante su elaboración.

Presentación del Plan de Seguridad Informática

La página inicial (portada) contiene el título siguiente: "**PLAN DE SEGURIDAD INFORMÁTICA**" seguido de la denominación de la entidad. En la segunda página se consignan los datos referidos a la elaboración, revisión y aprobación del Plan de Seguridad Informática, de acuerdo con el formato siguiente:

	Elaborado	**Revisado**	**Aprobado**
Nombre			
Cargo			
Firma			
Fecha			

En la columna "**elaborado**" se consignan los datos de la persona que dirigió el equipo que confeccionó el Plan de Seguridad Informática, en la columna "**revisado**" los de la persona designada para su revisión antes de presentarlo a aprobación y en la columna "**aprobado**" se reflejan los datos del jefe de la entidad en la que el Plan tiene vigencia.

Estructura del Plan de Seguridad Informática

Los componentes del PSI se estructuran de la forma siguiente:

1. Alcance del PSI.
2. Caracterización del Sistema Informático.
3. Resultados del análisis de riesgos.
4. Políticas de Seguridad Informática.
5. Responsabilidades.
6. Medidas y Procedimientos de Seguridad Informática
   6.1. Clasificación y control de los bienes informáticos.
   6.2. Del Personal.
   6.3. Seguridad Física y Ambiental.
   6.4. Seguridad de Operaciones.
   6.5. Identificación, Autenticación y Control de Acceso.
   6.6. Seguridad ante Programas Malignos.
   6.7. Respaldo de la Información.
   6.8. Seguridad en Redes.
   6.9. Gestión de Incidentes de Seguridad.

7. Anexos del Plan de Seguridad informática.
   7.1. Listado nominal de usuarios.
   7.2. Registros.
   7.3. Control de cambios.

1. Alcance del Plan de Seguridad Informática

El primer asunto que se define en el PSI es su espacio de aplicación, o sea su alcance. El alcance expresa el radio de acción que abarca el Plan, de acuerdo con el Sistema Informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el Sistema de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo de este) consiste en que permite tener, a priori, una idea precisa de la extensión y los límites en que este tiene vigencia.

A modo de ejemplo, la definición del alcance del PSI en una entidad hipotética (Empresa X) podría ser:

"El presente Plan de Seguridad Informática es aplicable en su totalidad en las áreas de la Oficina Central de la Empresa X que se encuentran en el edificio situado en la calle Martí No. 610, entre Céspedes y Agramonte, La Habana.

Las políticas expresadas en este plan son de obligatorio cumplimiento para todo el personal de la Empresa X, incluyen los de sus dependencias que se encuentran en los municipios Plaza, Playa y Cerro".

2. Caracterización del Sistema Informático

Se describe de manera detallada el sistema informático de la entidad, precisan los elementos que permitan identificar sus particularidades y las de sus principales componentes: la información, las tecnologías de información, las personas y los inmuebles, y se considera entre otros:

1. Bienes informáticos, su destino e importancia.
2. Redes instaladas, estructura, tipo y plataformas que utilizan.
3. Aplicaciones en explotación.
4. Servicios informáticos y de comunicaciones disponibles.
5. Características del procesamiento, transmisión y conservación de la información, se tiene en cuenta el flujo interno y externo y sus niveles de clasificación.
6. Características del personal vinculado con las tecnologías y sus servicios, en particular su preparación, profesionalidad y experiencia.
7. Condiciones de las edificaciones, su ubicación, estructura, disposición de los locales y condiciones constructivas.

Al describir el sistema informático se emplean los esquemas, tablas, gráficos y otros medios auxiliares que se requieran; a fin de facilitar una mejor comprensión. Estos medios auxiliares pueden ser insertados, dentro de esta propia sección o al final del plan, como anexos a los cuales se hace obligada referencia.

La caracterización del sistema informático permite conocerlo con plenitud, facilita una mejor determinación de las necesidades de protección y evita pérdida de tiempo e imprecisiones. Su descripción en detalle posibilita al que la lea tener un conocimiento lo más exacto posible de este, aunque sea la primera vez que se enfrente a él, cuestión que es de gran utilidad cuando se producen cambios en el personal, lo que suele ocurrir con relativa frecuencia.

Un ejemplo de caracterización del sistema informático de la Empresa X podría ser:

"El sistema informático de la Empresa X está soportado en los medios informáticos que se describen en el Anexo No. 1, que incluyen servidores, computadoras de mesa y portátiles, gran parte de ellas conectadas en red.

En la Oficina Central existe una red local que abarca las áreas situadas en la planta baja y los pisos 4 y 5 del edificio de la calle Martí No. 610.

Para la gestión de la red se cuenta con 5 servidores que utilizan como sistema operativo Windows 2003 Enterprise y Linux Debian; en las estaciones de trabajo se emplea Windows XP y Linux Ubuntu.

Los servidores tienen la función de: controlador de dominio, aplicaciones, base de datos, correo electrónico y Proxy.

Los servicios implementados en la red son navegación Internet, correo electrónico y transferencia de ficheros. La navegación y el correo tienen alcance nacional o internacional en dependencia de lo aprobado para cada usuario a partir de sus necesidades.

Las aplicaciones y bases de datos en explotación son:

- Sistema de Representación Geoespacial (SIRGE)
- Sistema Contable (CONTAB)
- Sistema de Control de Información Clasificada (SCIC)
- Sistema de Control de Componentes (Everest)
- Sistema de Control de Actualizaciones (WSUS)

Además se utilizan los paquetes de Office y Open Office para la elaboración de informes y otros documentos, en las máquinas previstas para el trabajo interno.

El cableado de la red está soportado por cable UTP categoría 5, 100 Mbits, con topología estrella (Anexo 2), protegido con canaletas. Las estaciones de trabajo se agrupan por áreas y pisos a partir de conmutadores (switchs) capa 2.

Además se cuenta con un punto de acceso inalámbrico (Access Point) a la red de Internet en el salón de reuniones del quinto piso.

La conexión con el exterior se realiza con el uso de una línea arrendada de 1 Mbit conectada directamente al proveedor de servicios de Internet.

El intercambio de información tanto interna como externa se realiza básicamente a través del correo electrónico.

La información ordinaria de la Oficina Central se procesa en las estaciones de trabajo de la red y la información clasificada en máquinas independientes, ubicadas en la Dirección de la Empresa, en el Departamento de Cuadros y en el de Seguridad y Defensa. La información recibida desde las dependencias de la empresa y la que se envía al Organismo superior se tramita por medio del correo electrónico y de la Intranet. La información que se expone en la Intranet es en todos los casos de uso público.

El edificio de Martí 610 se encuentra cerca del litoral habanero, tiene buenas condiciones constructivas, adecuadas tanto para la protección como para la preservación de los equipos y la posibilidad de visibilidad de las pantallas desde el exterior es prácticamente nula.

El personal que opera los equipos posee los conocimientos y la preparación necesaria para su empleo y en la mayor parte de los casos tiene nivel medio o superior."

3. Resultados del análisis de riesgos

Una vez definido el alcance del PSI y realizada una detallada descripción del sistema informático, corresponde finalizar esta primera parte con la formulación de las conclusiones obtenidas durante la determinación de las necesidades de protección, mediante la evaluación de los riesgos. Estas conclusiones incluyen:

a) Cuáles son los bienes informáticos más importantes para la gestión de la entidad y por lo tanto requieren de una atención especial desde el punto de vista de la protección; se especifican aquellos considerados de importancia crítica por el peso que tienen dentro del sistema;
b) qué amenazas pudieran tener un mayor impacto sobre la entidad en caso de materializarse sobre los bienes a proteger;
c) cuáles son las áreas con un mayor peso de riesgo y qué amenazas lo motivan.

Un ejemplo de los resultados del análisis de riesgos en la Empresa X podría ser:

Los bienes informáticos más importantes a proteger son:

- La red de trabajo interno de la Oficina;
- El servidor de aplicaciones;
- Las bases de datos del sistema SIRGE (de importancia crítica);
- Las bases de datos de la intranet;
- El servicio de correo electrónico;
- El sistema contable CONTAB.

Las amenazas más importantes a considerar de acuerdo con el impacto que pudieran tener sobre la empresa son:

- El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- Pérdida de disponibilidad.
- La sustracción, alteración o pérdida de datos.
- Fuga de información clasificada.
- La introducción de programas malignos.
- El empleo inadecuado de las tecnologías y sus servicios.
- Las penetraciones del mar.

Las áreas sometidas a un mayor peso/riesgo y las amenazas que lo motivan son:

- El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).
- El local de Economía (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).
- El Departamento de Investigación y Desarrollo (alteración o pérdida de datos, pérdida de disponibilidad y la introducción de programas malignos).
- Las oficinas de la Dirección, del Departamento de Cuadros y del Departamento de Seguridad y Defensa (fuga de información clasificada).
- El almacén situado en la planta baja del edificio (penetraciones del mar).

En la medida en que las conclusiones del análisis de riesgos sean más precisas se logra una visión más acertada de hacia dónde son dirigidos los mayores esfuerzos de seguridad y por supuesto los recursos disponibles para ello, y se logra que esta sea más rentable.

4. Políticas de Seguridad Informática

En esta sección se definen los aspectos que conforman la estrategia a seguir por la Entidad sobre la base de sus características, de conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado.

Establecen las normas generales que cumple el personal que participa en el sistema informático y se derivan de los resultados obtenidos en el análisis de riesgos y de las definidas por las instancias superiores en las leyes, resoluciones, reglamentos, y otros documentos rectores.

Al definir las políticas de Seguridad Informática que son establecidas en la entidad se consideran los elementos expuestos en el punto No. 1.4.1 de la Primera Parte de esta Metodología.

Las políticas que se describan comprenden toda la organización, ya que es obligatorio su cumplimiento en las áreas que las requieran, razón por las que son lo suficientemente generales y flexibles para poder implementarse, en cada caso, mediante las medidas y procedimientos que demanden las características específicas de cada lugar.

A modo de ejemplo se muestran algunas de las políticas definidas en la Empresa X:

1. Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprueban por el Consejo de Dirección.
2. El acceso a las tecnologías de la entidad es expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la seguridad informática.
3. Los usuarios de las tecnologías de la información y la comunicación responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su Jefe inmediato superior.
4. Todos los bienes informáticos son identificados y controlados físicamente hasta nivel de componentes.
5. Se establecen procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.
6. Se prohíbe vincular cuentas de correo electrónico de la entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través de este.
7. En caso de violación de la seguridad informática, se comunica al Jefe inmediato superior y a la Oficina de Seguridad para las Redes Informáticas y se crea una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.

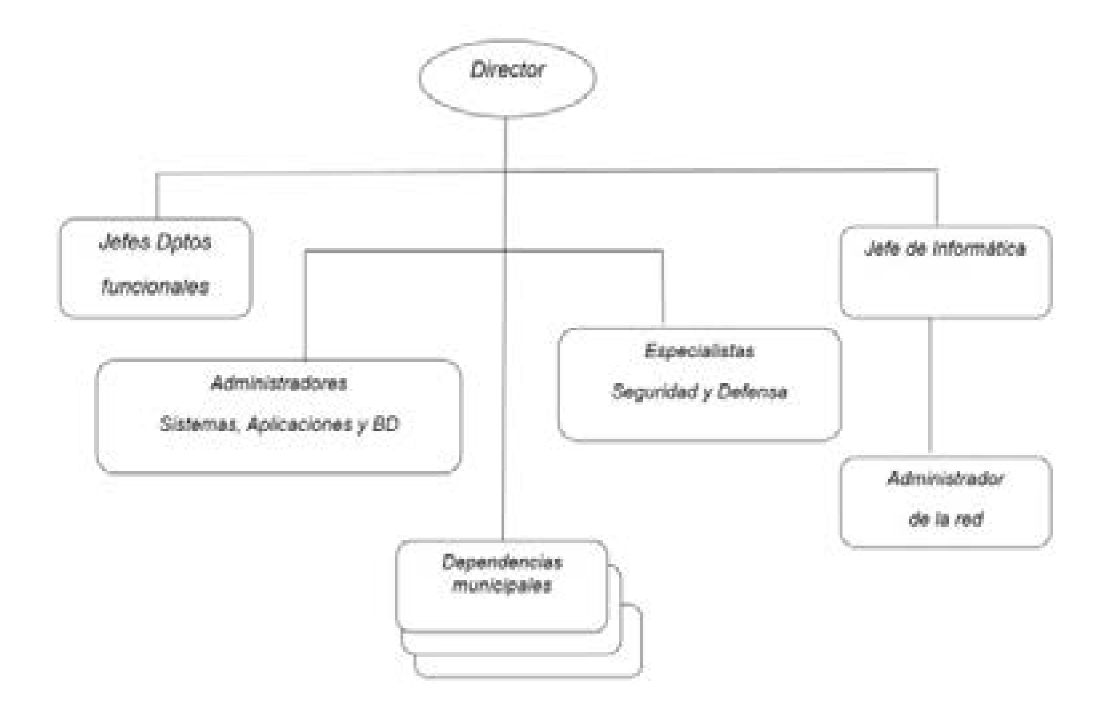
5. Responsabilidades

Se describe la estructura concebida en la Entidad para la gestión de la Seguridad Informática, se especifican las atribuciones, funciones y obligaciones de las distintas categorías de personal, que incluyen: directivos a los distintos niveles (jefe de la entidad, jefes de departamentos, áreas y grupos de trabajo o estructuras equivalentes); jefes y especialistas de informática; administradores de redes, sistemas y aplicaciones; especialistas de seguridad informática y de seguridad y protección y usuarios comunes de las tecnologías de Información.

Al especificar las atribuciones, funciones y obligaciones del personal en función de sus cargos, se tiene en cuenta lo establecido al respecto en el Reglamento de Seguridad para las TIC.

Un ejemplo de la estructura concebida para la gestión de la seguridad informática y de las funciones y obligaciones de los administradores de sistemas, aplicaciones y bases de datos en la Empresa X podría ser:

Estructura de gestión de la seguridad informática de la Empresa



Funciones y Obligaciones de los Administradores de Sistemas, Aplicaciones y Bases de Datos de la Empresa X.

a) Informar a los usuarios de los controles de seguridad que hayan sido establecidos y verificar su utilización apropiada;
b) controlar el acceso a los sistemas, aplicaciones y bases de datos en correspondencia con la política establecida;
c) garantizar la ejecución de los procedimientos de salva de programas y datos, así como su conservación;
d) detectar posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y proponer acciones para su solución;
e) garantizar su mantenimiento y actualización y el registro de los sistemas y aplicaciones que lo requieran.

Aplicaciones, Sistemas y Bases de Datos	*Administrador (poner nombres)*
Sistema de Representación Geoespacial (SIRGE)	*Jesús*
Sistema de Control de Componentes (Everest)	*Julio*
Sistema contable CONTAB	*Anaibis*
Sistema de control información clasificada (SCIC)	*Diana*
Sistema de Control de Actualizaciones (WSUS)	*Humberto*

6. Medidas y Procedimientos de Seguridad Informática

En este segmento del PSI se describe **cómo** se implementan, en las áreas a proteger, las políticas que han sido definidas para la entidad, en correspondencia con las necesidades de protección en cada una de ellas, de acuerdo con sus formas de ejecución, periodicidad, personal participante y medios. Se describen por separado los controles de seguridad implementados, en correspondencia con su naturaleza, se combinan el empleo de los recursos humanos y de los medios técnicos con las acciones que son realizadas.

Las medidas y procedimientos no deben confundirse con una declaración de intención o línea de deseos, por lo que con su descripción se especifican los controles implementados, no los que se quisieran implementar.

El PSI se sustenta sobre la base de los recursos disponibles y en dependencia de los niveles de seguridad alcanzados y de los aspectos que queden por cubrir se elabora un Programa de Desarrollo de la Seguridad Informática, que incluya las acciones a realizar por etapas para lograr niveles superiores (ver punto No. 2.1. de la Primera Parte).

Hay que concentrarse en las acciones que garantizan la instrumentación de las políticas definidas y su aplicación apropiada en cada área que lo requiere.

6.1. Clasificación y control de los bienes informáticos

Estas medidas y procedimientos persiguen identificar los bienes informáticos de acuerdo con su importancia, controlar y supervisar que sean utilizados en funciones propias del trabajo y garantizar su protección. En este apartado se incluyen las medidas y los procedimientos que se requieran para:

1. Precisar los métodos de supervisión y control que se utilicen, el personal encargado de ejecutarlos y los medios empleados para ello.
2. Establecer los mecanismos que se requieran para identificar y controlar los bienes informáticos y la conformación de su inventario permanentemente actualizado.
3. Precisar la persona encargada de cada bien informático y responsable por su protección.
4. Garantizar la autorización y el control sobre el movimiento de los bienes informáticos.

A modo de ejemplo de medidas y procedimientos de control de los medios informáticos se muestran los siguientes:

Medida:

La administradora del sistema CONTAB responde por la integridad de los medios destinados para la explotación de esta aplicación.

Procedimiento 1 Control de medios informáticos.

1. Acceder la última semana de cada mes al Sistema de Control de Componentes (Everest) a través del servidor de la red y se aplica a los medios informáticos que forman parte del dominio de la red.
2. Comprobar cambios existentes desde el último control realizado.
3. Informar a la Dirección de la Empresa los resultados de la comprobación.
4. Generar un resumen de los resultados de cada control y conservarlo por un año.
   Responsable: *Administrador de la red*
5. Esclarecer en caso de existir diferencia, las causas y responsabilidades.
   Responsable: Director de la empresa

6.2. Del Personal

Las medidas y procedimientos asociadas con el personal tienen como objetivo garantizar el cumplimiento de las funciones y responsabilidades de seguridad generales y específicas de las personas vinculadas con las TIC y sus servicios, así como la documentación de estas y aseguran:

1. La selección adecuada del personal previsto para ocupar cargos en la actividad informática o con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas.
2. La obligación de la entidad en cuanto a la preparación del personal y la responsabilidad del trabajador hacia la Seguridad Informática, así como la inclusión de estos aspectos en los términos y condiciones del contrato de empleo.
3. La forma en que es autorizada por la dirección de la entidad la utilización de las tecnologías y sus servicios por parte de los usuarios que lo necesiten.
4. La obligación de los jefes a cada nivel en cuanto a garantizar la Seguridad Informática en su área de responsabilidad.
5. Las acciones a realizar en caso de empleo no autorizado de las tecnologías y sus servicios por parte de los usuarios.
6. La responsabilidad de los jefes a cada nivel en cuanto a la preparación de su personal y del conocimiento de sus deberes y derechos, incluyen la introducción en el contrato de trabajo de la constancia del compromiso de cada trabajador.
7. Los requerimientos de seguridad para la autorización del acceso a las tecnologías y servicios por parte de personal externo.
8. Las formas y medios mediante los cuales los usuarios informan acerca de cualquier incidente de seguridad, debilidad o amenaza.
9. Evitar la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, así como la introducción, ejecución, distribución o conservación de programas para esos fines o información contraria al interés social, la moral y las buenas costumbres.

Los controles de seguridad en relación con el personal consideran no solo los requisitos a cumplir por los trabajadores durante el tiempo de vigencia de su contrato de empleo, sino también antes de ser contratado y con posterioridad al cese de su relación laboral.

Un ejemplo de procedimiento relacionado con el personal en la Empresa X podría ser:

Procedimiento 2 Aprobación de acceso a las tecnologías y servicios por parte de personal externo.

1. Elaborar y presentar la solicitud de autorización de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos de la persona que necesita el acceso y su número de carné de identidad; las razones que justifican este acceso, el acceso que se requiere y el tiempo que se requiera mantenerlo.
   Responsable: Jefe del área asociada con el acceso
2. Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red, al Jefe del área que realizó la solicitud y al Jefe del Departamento de Seguridad y Defensa, especifican el alcance del acceso y su tiempo de vigencia.
   Responsable: Director de la Empresa

3. Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor de la red los atributos en correspondencia con la autorización otorgada.
   Responsable: Administrador de la red
4. Imponer a la persona a que se otorga el acceso de sus obligaciones y atribuciones en relación con el empleo de las tecnologías y sus servicios.
   Responsable: Jefe del área que solicita el acceso
5. Solicitar al director la cancelación del acceso concedido e informar las razones de la solicitud.
   Responsable: Jefe del área que solicita el acceso
6. Cancelar la cuenta y los permisos de acceso una vez concluido el plazo previsto.
   Responsable: Administrador de la red.

6.3. Seguridad Física y Ambiental

Las medidas y procedimientos de seguridad física y ambiental tienen como objetivo evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones, las tecnologías y la información de la organización.

Se aplican a los locales donde se encuentran las TIC y directamente a estas mismas tecnologías y a los soportes de información e incluyen: medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.

La protección física se alcanza con la creación de una o más barreras físicas alrededor de las áreas de procesamiento de la información. El uso de múltiples barreras brinda protección adicional, de modo que la falta de una barrera no significa que la seguridad se vea comprometida inmediatamente.

La protección del equipamiento (incluyen aquel utilizado fuera de la entidad) es necesaria para reducir el riesgo de accesos no autorizados a la información y para protegerlo contra pérdidas o daños. Se pueden requerir controles especiales para proteger contra amenazas físicas, y para preservar los equipos, tales como la garantía del suministro eléctrico y la infraestructura adecuada del cableado.

La seguridad ambiental incluye la aplicación de medios contra daños que puedan ser ocasionados por incendios, inundaciones, terremotos, explosiones, perturbación del orden, y otras formas de desastre natural o artificial.

Las medidas y procedimientos de seguridad física y ambiental van dirigidas a:

1. La protección de las tecnologías contra la sustracción o alteración, e incluyen sus componentes y la información que contienen.
2. Impedir su empleo para cometer acciones malintencionadas o delictivas.
3. Disminuir el impacto producido por fuego, inundación, explosión, perturbación del orden y otras formas de desastre natural o artificial.
4. La protección contra fallas de alimentación u otras anomalías eléctricas.
5. La protección de los cables que transporten datos o apoyen los servicios contra la intercepción o el daño.
6. Garantizar que el equipamiento reciba un mantenimiento adecuado en correspondencia con las especificaciones del fabricante.
7. El control del movimiento de las tecnologías.
8. La preservación de la información del equipamiento que cause baja o se destine a otras funciones.

Corresponde a esta parte del PSI la determinación de los locales considerados como áreas o zonas controladas, en correspondencia con la caracterización del sistema informático realizado y los resultados del análisis de riesgos y que por lo tanto tienen requerimientos específicos de seguridad, en base a lo cual se declaran áreas **limitadas, restringidas o estratégicas** y se describen las medidas que se aplican en cada una de ellas, por ejemplo: restricciones para limitar el acceso a los locales, procedimientos para el empleo de cierres de seguridad y dispositivos técnicos de detección de intrusos y otros.

Al referir las medidas y procedimientos que se establecen para lograr una seguridad física y ambiental adecuada a las necesidades de las TIC, no es necesario describir las condiciones constructivas de los inmuebles, pues ya eso ha sido realizado durante la caracterización del sistema informático y expuesto en el punto 2 de la estructura del PSI.

Un ejemplo de la clasificación y medidas específicas en las áreas controladas en la Empresa X es la siguiente:

Área controlada	***Categoría***	***Medidas específicas***
Dirección, Cuadros, Seguridad y Defensa	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos.*
Economía	*Limitada*	*Acceso físico limitado; control de soportes removibles; alarma contra intrusos; separación de funciones; protección de las copias de programas y datos.*
Servidores de la red	*Limitada*	*Acceso solo a administradores; cierre magnético en la puerta de acceso y alarma contra intrusos: redundancia de HW, SW, climatización y datos.*
Investigación y Desarrollo	*Limitada*	*Acceso físico limitado; cierres seguros en puertas y ventanas; alarma contra intrusos; redundancia de datos.*

Se describen en detalle las medidas específicas de la tercera columna de la tabla anterior: a quien se autoriza el acceso, tipo de alarma, en que consiste el cierre seguro, como se controlan los soportes removibles, qué funciones están separadas en usuarios diferentes, cómo se logra la redundancia y la protección de la información de respaldo y otros.

Obsérvese que las áreas declaradas como controladas coinciden con las que se determinó en el análisis de riesgos que estaban sometidas a un mayor peso de riesgo (ver punto 3 de la estructura del PSI, Resultados del análisis de riesgos).

En el próximo ejemplo se muestra una medida con el procedimiento correspondiente para el control del movimiento de las tecnologías:

Medida:

La entrada, salida y traslado de las TIC en la Empresa X se realiza con autorización del Director en correspondencia con el Procedimiento 3, dejan constancia de ello en el Registro 1, movimiento de TIC.

Procedimiento 3 Movimiento de las TIC

1. Solicitar autorización por escrito al Director de la Empresa X para el movimiento de las tecnologías que lo requieran, fundamentan en qué consiste el movimiento, los motivos y si es temporal el tiempo requerido.

   Responsable: Jefe del área a que pertenece el medio a trasladar

2. Autorizar si es procedente el movimiento de las tecnologías y darlo a conocer por escrito al Jefe del área que realizó la solicitud, al Jefe del área de Contabilidad y al Jefe del Departamento de Seguridad y Defensa, especifican el tiempo de vigencia de la autorización.
   Responsable: Director de la Empresa X
3. Registrar en el sistema CONTAB el movimiento del medio básico autorizado a trasladar.
   Responsable: Jefe del área de Contabilidad.
4. Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a trasladar, precisan la existencia y estado de sus partes y componentes, si contienen información y de qué tipo, así como lo relacionado con el control antivirus.
   Responsable: *Jefe del área a que pertenece el medio a trasladar*
5. Consignar el movimiento en el Registro 1, especifican la fecha en que se produce, los datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento (evento, exposición, reparación y otros).
   Responsable: Jefe del área a que pertenece el medio a trasladar
6. *Controlar el cumplimiento de las autorizaciones sobre el movimiento de las tecnologías y su registro adecuado.*
   Responsable: Jefe del Departamento de Seguridad y Defensa

6.4. Seguridad de Operaciones

Las medidas y procedimientos de Seguridad de Operaciones están dirigidas a lograr una eficiente gestión de la seguridad y garantizan el cumplimiento de las regulaciones vigentes en el país, así como las establecidas por la propia entidad.

La gestión del sistema de seguridad implica el control de las acciones que se realizan dentro del sistema informático y su garantía de que se ajustan a las políticas de seguridad establecidas para el empleo de las tecnologías y sus servicios, y para ello las medidas y procedimientos de seguridad de operaciones consideran, entre otros, los aspectos siguientes:

1. La aplicación del principio de separación de funciones evita que se asignen a una misma persona tareas que en su conjunto pueden propiciar la modificación no autorizada de datos o el mal uso de los sistemas.
2. La aprobación para la introducción en la entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones, previa verificación de su correspondencia con el sistema de seguridad establecido y el cumplimiento de los criterios de seguridad apropiados.
3. El control por el personal autorizado de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores de los sistemas, su documentación y reporte a quienes corresponda.

En esta parte del PSI se incluye la ejecución de los procedimientos de revisión mediante los métodos de medición que posibiliten detectar errores de proceso, identificar fallos de seguridad de forma rápida y determinar las acciones a realizar para lograr el ciclo de mejora continua. Se utilizan para ello los indicadores seleccionados sobre la base de los criterios respecto a qué aspectos se controlan y miden para lograr el cumplimiento de los objetivos planteados en el SGSI implementado en la entidad. Existen diversos métodos de medición y hay disponibles diferentes procedimientos y herramientas que facilitan su implementación en cualquier entidad (ver punto 3 de la Primera Parte, Proceso de Verificación del SGSI).

Se incluyen además las medidas y procedimientos implementados para el registro y análisis de las trazas de auditoría generadas por los sistemas operativos y servicios de redes, y por los sistemas instalados según lo reglamentado, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios y otros), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

En caso de empleo de software especializado que permita la detección de posibles errores de configuración u otras vulnerabilidades, así como su corrección, se describen los procedimientos requeridos.

Se refieren además las medidas que garanticen la integridad de los mecanismos y registros de auditoría limitan su acceso solo a las personas autorizadas para ello.

A modo de ejemplo de procedimiento de las acciones necesarias para cubrir las brechas de seguridad y la corrección de los errores en la Empresa X se muestra el siguiente:

Procedimiento 4 Corrección de errores y brechas de seguridad.

1. Instalar y configurar las aplicaciones Wsus, destinada para distribuir parches de seguridad de Microsoft para la eliminación de vulnerabilidades conocidas cuando su solución sea publicada por el fabricante y LANguard y Nmap, para detectar brechas de seguridad, puertos abiertos y otras vulnerabilidades similares.
   Responsable: Administrador de la red
2. Ejecutar las aplicaciones LANguard y Nmap una vez al mes y controlar cada lunes la ejecución de Wsus.
   Responsable: Administrador de la red
3. Informar los resultados de las acciones de corrección de errores y brechas de seguridad al Jefe del Departamento de Informática cada vez que se realicen y preservar los registros en los soportes habilitados al efecto por un tiempo no menor de un año.
   Responsable: Administrador de la red
4. Analizar los resultados de las acciones de corrección de errores y brechas de seguridad y su correspondencia con lo previsto en el Sistema de Seguridad Informática de la Empresa y, en caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.
   Responsable: Jefe del Departamento de Informática
5. Actualizar los cambios en el PSI.
   Responsable: Jefe del Departamento de Informática

6.5. Identificación, Autenticación y Control de Acceso

Las medidas y procedimientos de identificación, autenticación y control de acceso responden a las políticas que previamente fueron definidas en la entidad sobre estos aspectos, y tienen como objetivo gestionar el acceso a la información de forma segura, garantizan el acceso de usuarios autorizados e impiden el acceso no autorizado a los sistemas de información. Los accesos a la información y a las instalaciones de procesamiento de la información son controlados sobre la base de requisitos de seguridad. Los controles consideran:

a) Las políticas para la autorización y distribución de la información.
b) La consistencia entre los controles de acceso y las políticas de clasificación de la información.
c) La legislación vigente y las obligaciones contractuales con respecto a la protección del acceso a los datos o servicios.
d) El establecimiento de perfiles estándar es de acceso de usuarios para roles comunes.
e) La gestión de derechos de acceso en un ambiente distribuido y de redes, que reconozca todos los tipos de conexión posibles.
f) La separación de roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso y administración de acceso.
g) Los requisitos para autorizaciones formales de solicitudes de acceso.
h) La cancelación de derechos de acceso.

Esos controles cubren todas las etapas del ciclo de vida del acceso del usuario, desde el registro inicial de nuevos usuarios hasta la cancelación final del registro de usuarios que no requieren más acceso a los sistemas de información y a los servicios.

Identificación de usuarios

Los procedimientos de identificación de usuarios garantizan:

a) la utilización de un identificador único (ID) para cada usuario para permitir que queden vinculados y sean responsables de sus acciones;
b) la verificación de que el usuario tenga autorización para el uso del servicio o el sistema de información;
c) la verificación de que el nivel de acceso otorgado se corresponda con la necesidad de uso y que es consistente con la política de seguridad, por ejemplo que no compromete la segregación de tareas;
d) que los usuarios firmen declaraciones indica que ellos comprenden y asumen las condiciones de acceso;
e) mantener un registro impreso de todas las personas a las que se les otorga acceso;
f) eliminar inmediatamente o bloquear los derechos de acceso de los usuarios que hayan cambiado roles o tareas o dejado la organización; y
g) realizar periódicamente una verificación para eliminar o bloquear las cuentas e identificadores de usuarios (ID´s) redundantes.

Se explica el método empleado para la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes, y se especifica:

1. Cómo se asignan los identificadores de usuarios.
2. Si existe una estructura estándar para la conformación de los identificadores de usuarios.
3. Quién asigna los identificadores de usuarios.
4. Cómo se eliminan los identificadores de usuarios una vez que concluya la necesidad de su uso y cómo se garantiza que estos no sean utilizados nuevamente.
5. El proceso de revisión de utilización y vigencia de los identificadores de usuarios asignados.

Autenticación de usuarios

Se explica el método de autenticación empleado para comprobar la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes.

Cuando se utilice algún dispositivo específico de autenticación, se describe su forma de empleo. En el caso de empleo de autenticación simple por medio de contraseñas se especifica:

1. Cómo son establecidas las contraseñas.
2. Tipos de contraseñas utilizadas (configuración de arranque, protector de pantalla, aplicaciones).
3. Estructura y periodicidad de cambio que se establezca para garantizar la fortaleza de las contraseñas utilizadas en los sistemas, servicios y aplicaciones, en correspondencia con el peso de riesgo estimado para estos.
4. Causas que motivan el cambio de contraseñas antes de que concluya el plazo establecido.

La estructura y periodicidad de cambio de las contraseñas de acceso son seleccionadas en correspondencia con la importancia de los bienes cuyo acceso se protege y los riesgos a que están sometidos, así como la existencia de otros tipos de controles complementarios que contribuyan a su protección, por lo que no necesariamente son iguales en todos los casos. Por ejemplo, para un sistema que no está catalogado como de importancia crítica para la entidad y que además está ubicado en un área a la que no acceden muchas personas, tal vez una contraseña de pocos caracteres que se modifique en intervalos largos sería suficiente, por el contrario un sistema de importancia crítica para la entidad cuenta con contraseñas de mayor fortaleza, se obliga a su cambio con mayor frecuencia.

En una red, con este objetivo podrían crearse grupos con necesidades de seguridad comunes, a los cuales se les impondrían requerimientos diferenciados en cuanto a la estructura y cambio de las contraseñas de acceso.

La instauración de contraseñas se controla a través de un proceso formal de gestión. El proceso incluye los requisitos siguientes:

a) Exigir a los usuarios que firmen una declaración de que se comprometen a mantener confidencialidad sobre las contraseñas personales; esta declaración firmada se incluye dentro de los términos de empleo como parte de sus responsabilidades hacia la Seguridad Informática (ver punto 6.2 “Del Personal”);
b) establecer procedimientos para verificar la identidad del usuario antes de la utilización de cualquier contraseña;
c) cuando se asigne inicialmente una contraseña temporal, los usuarios son forzados a cambiarla inmediatamente después del primer acceso;
d) las contraseñas temporales son proporcionadas a los usuarios de un modo seguro y se evita el uso de mensajes de correo electrónico de terceras partes o no protegidos (en texto claro);
e) las contraseñas por defecto de los vendedores se cambian inmediatamente luego de la instalación del software o sistemas; y
f) las contraseñas son únicas para cada persona y no son descifrables.

Las contraseñas son un medio común de verificación de la identidad del usuario antes de acceder a los sistemas de información o a los servicios, de acuerdo con la autorización que tenga el usuario, pero es un método que puede ser violado con relativa facilidad. En los casos que se requiera una mayor seguridad, se consideran otras tecnologías disponibles para la identificación y autenticación del usuario, tales como biometría, por ejemplo, verificación de huella digital, verificación de firma, y uso de medios físicos de autenticación como tarjetas inteligentes.

Se exige a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios son advertidos en cuanto a:

a) Mantener confidencialidad sobre la contraseña;
b) evitar mantener un registro de contraseñas en texto claro en cualquier medio (por ejemplo, papel, archivo de software o dispositivo de mano);
c) cambiar las contraseñas cuando haya una indicación de riesgo en el sistema o en la contraseña;
d) seleccionar contraseñas de calidad con suficiente longitud mínima que sean:
   1. Fáciles de recordar.
   2. No se basen en algo que alguien pueda adivinar fácilmente o usen información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc.
   3. No vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios).
   4. Libres de caracteres idénticos sucesivos ya sean numéricos o alfabéticos.
e) Cambiar las contraseñas a intervalos regulares o basados en el número de accesos (las contraseñas de cuentas privilegiadas son cambiadas más frecuentemente que las contraseñas normales), y evitar la reutilización o reciclaje de contraseñas;
f) cambiar las contraseñas temporales en la primera conexión;
g) no incluir contraseñas en ningún proceso automatizado de conexión;
h) no compartir las contraseñas de usuario individuales; y
i) no utilizar la misma contraseña para propósitos de trabajo y particulares.

Control de acceso a los bienes informáticos

Se describen las medidas y procedimientos que aseguran el acceso autorizado a los bienes informáticos que requieren la imposición de restricciones a su empleo, se especifica:

1. A qué bienes informáticos se le implementan medidas de control de acceso.
2. Métodos de control de acceso utilizados.
3. Quién otorga los derechos y privilegios de acceso.
4. A quién se otorgan los derechos y privilegios de acceso.
5. Cómo se otorgan y suspenden los derechos y privilegios de acceso.

El control de acceso a los bienes informáticos está basado en una política de "mínimo privilegio", en el sentido de otorgar a cada usuario solo los derechos y privilegios que requiera para el cumplimiento de las funciones que tenga asignadas.

La asignación de derechos y privilegios es controlada a través de procedimientos formales de autorización que determinan el perfil de cada usuario. Se consideran los elementos siguientes:

a) Asociar el derecho de acceso con cada componente, por ejemplo sistema operativo, sistema de gestión de base de datos y de cada aplicación, identifican los usuarios a los que es necesario asignar tales privilegios;
b) los privilegios son asignados sobre la base de necesidad de uso y consideran recurso por recurso;
c) se implementa un proceso de autorización y se mantiene un registro de todos los privilegios asignados; los privilegios no se otorgan hasta que el procedimiento de autorización concluya.

Hay que tener en cuenta que el uso inapropiado de los privilegios de administración puede ser un factor importante de surgimiento de fallas o brechas de seguridad (cualquier característica o recurso de un sistema informático que habilite al usuario a hacer caso omiso de los controles de este o de la aplicación).

La dirección de la entidad instrumenta la revisión de los derechos de acceso de los usuarios a intervalos regulares para mantener un control efectivo sobre el acceso a los datos y servicios informáticos, utilizan un proceso formal que considere los siguientes aspectos:

a) Los derechos de acceso de usuarios son revisados después de cualquier cambio, tal como el traslado de un cargo a otro dentro de esta organización, o el cese de las relaciones laborales; y

b) verificar que con la asignación de derechos no se obtienen privilegios no autorizados.

Como parte del control de acceso a los bienes informáticos se incluyen las medidas y procedimientos establecidos, con el fin de evitar la modificación no autorizada, destrucción y pérdida de los ficheros y datos, así como para impedir que sean accedidos públicamente, se especifican:

1. Medidas de seguridad implementadas a nivel de sistemas operativos, aplicación o ambos, para restringir y controlar el acceso a las bases de datos.
2. Medidas para garantizar la integridad del software y la configuración de los medios técnicos.
3. Empleo de medios criptográficos para la protección de ficheros y datos.

Ejemplo de procedimiento en la Empresa X

Procedimiento 5 Aprobación y cancelación de acceso a las TIC

1. Elaborar y presentar la solicitud de autorización (cancelación) de acceso a las TIC al Director de la Empresa, donde se incluya el nombre y apellidos del trabajador que necesita el acceso; las razones que justifican este acceso y los activos a que solicita acceder. De ser una necesidad temporal especifica el tiempo que se requiera mantenerlo. En el caso de retiro del acceso presenta breve informe que refiere los motivos de la propuesta y si es definitiva o temporal.
   Responsable: Jefe del área a que pertenece el trabajador
2. Aprobar (denegar) la solicitud en caso que corresponda, y darlo a conocer por escrito al administrador de la red y al Jefe del área que realiza la solicitud, especifica el alcance del acceso.
   Responsable: Director de la Empresa
3. Preparar al trabajador en el uso adecuado de las TIC y en sus obligaciones como usuario de estas y firma por el trabajador del compromiso de empleo de estas. El documento original se entrega al administrador de la red y la copia se incluye en el contrato de trabajo.
   Responsable: Jefe del área a que pertenece el trabajador
4. Asignar (en caso de autorización de acceso), un identificador personal y único para el acceso a los sistemas y servicios determinados en la aprobación y definir en el servidor los atributos en correspondencia con la autorización otorgada.
   Responsable: Administrador de la red
5. Otorgar al usuario una contraseña temporal para ser utilizada en su primera conexión, se obliga a cambiarla una vez que acceda al sistema o servicio asignado.
   Responsable: Administrador de la red
6. Configurar en el servidor los atributos que se determinen o se agregan en correspondencia con la autorización otorgada.
   Responsable: Administrador de la red
7. Cancelar, en caso de revocación de acceso, la cuenta y los permisos de acceso otorgados.
   Responsable: Administrador de la red

8. Conservar las autorizaciones de acceso a las TIC en el área de informática por un período no menor de 1 año.
   Responsable: Jefe del Departamento de Informática
9. Realizar un control trimestral de este procedimiento e informar de sus resultados al Director de la Empresa.
   Responsable: Jefe del Departamento de Organización y Supervisión

6.6. Seguridad ante programas malignos

Se establecen las medidas y procedimientos que se requieran para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, se especifican los programas antivirus utilizados y su régimen de instalación y actualización.

La protección contra códigos maliciosos se basa en el empleo de medidas de prevención, detección y recuperación, en la necesidad de la seguridad, y en controles apropiados de acceso al sistema. Las siguientes pautas son consideradas:

1. Establecimiento de políticas que instituyan la prohibición del uso de software no autorizado y la protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indican las medidas protectoras a adoptar.
2. Revisiones regulares del contenido de datos y software que soportan los procesos de gestión de la entidad y de la presencia de archivos no aprobados o modificaciones no autorizadas.
3. La instalación y actualización regular de programas antivirus que exploren las computadoras y los soportes de forma rutinaria o como un control preventivo para la detección y eliminación de código malicioso; las verificaciones incluyen:
   a) Comprobación de archivos en medios electrónicos u ópticos, y archivos recibidos a través de redes, para verificar la existencia de código malicioso, antes de su uso;
   b) comprobación de todo archivo adjunto a un correo electrónico o de cualquier descarga antes de su uso; realizar esta comprobación en distintos lugares, por ejemplo, en los servidores de correo, en las computadoras terminales o a la entrada de la red de la organización;
   c) comprobación de páginas Web para saber si existe en ellas código malicioso.
4. La definición de procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación para su uso, la información de los ataques de los virus y las acciones de recuperación.
5. La implementación de medidas para la recuperación ante ataques de código malicioso, incluyen los datos y software necesarios de respaldo y las disposiciones para la recuperación.
6. La implementación de procedimientos para obtener información sobre nuevos códigos maliciosos a través de listas de correo y comprobación de los sitios Web que brindan esa información.
7. La implementación de procedimientos para verificar la información relativa al software malicioso y asegurarse que es real; los encargados de esta actividad pueden diferenciar los códigos maliciosos reales de los falsos avisos de código malicioso, para lo que usan fuentes calificadas; se advierte al personal sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

Ejemplo de procedimiento en la Empresa X

Procedimiento 6 Descontaminación de programas malignos

1. Al detectar en una estación de trabajo indicios de contaminación detener la actividad que se realiza, desconectarla de la red e informar al Jefe inmediato y al Administrador de la red.

Responsable: Usuario de la estación de trabajo

2. Identificar de qué tipo de programa maligno se trata.
3. Verificar que en el medio contaminado se ejecuta una versión actualizada del programa antivirus instalado y de no cumplirse, proceder a la actualización del programa antivirus y llevar a cabo la descontaminación. De ser exitosa la descontaminación, poner en operación el medio afectado.
4. Revisar los soportes y el resto de las tecnologías que pudieran haber sido afectadas.
5. Investigar las causas de aparición del código malicioso.
6. Realizar las anotaciones pertinentes en el Registro de Incidencias (Registro No. 3).
7. Reportar el incidente a su instancia superior y a la OSRI.
8. Si es un programa maligno desconocido, proceder al aislamiento del fichero contaminado y remitirlo a la empresa Segurmática.

Responsable: Administrador de la red

6.7. Respaldo de la Información

Las medidas y procedimiento de respaldo que se implementen garantizan mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información frente a cualquier eventualidad.

Para alcanzar un nivel de respaldo adecuado se hacen las copias de seguridad de la información y del software que se determinen en cada caso y se comprueban regularmente. Se dispone de procedimientos de respaldo para asegurar que toda la información esencial y el software puedan recuperarse tras un desastre o fallo, considerar para ello los elementos siguientes:

a) Definir el nivel necesario de información de respaldo;

b) realizar copias seguras y completas de la información, y establecer los procedimientos de restauración;

c) determinar el grado (completo o parcial) y la frecuencia de los respaldos en correspondencia con los requisitos de la entidad, los requisitos de seguridad de la información implicada, y la importancia de la información que permita la operación continúa de la organización;

d) precisar las copias que son almacenadas en un área apartada del lugar habitual de procesamiento de la información que se preserva, a una suficiente distancia para la salvaguarda de cualquier daño producto de un desastre en el sitio principal;

e) establecer un nivel apropiado de protección ambiental y físico (ver punto 6.3. “Seguridad Física y Ambiental”) de la información de respaldo, consistente con las normas aplicadas en el sitio principal; los controles aplicados a los soportes en el sitio principal se extienden para cubrir el sitio de respaldo;

f) probar regularmente los soportes de respaldo para verificar que puede confiarse en ellos para el uso cuando sean necesarios;

g) comprobar regularmente los procedimientos de restauración para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos de recuperación; y

h) proteger los respaldos por medio del cifrado en los casos que se requiera.

Para los sistemas críticos, las disposiciones de respaldo cubren la información y datos para recuperar el sistema completo en caso de un desastre.

Los procedimientos de respaldo, cuando sea posible, se automatizan para facilitar el respaldo y los procesos de restauración. Tales soluciones automatizadas se prueban suficientemente, antes de la puesta en práctica y en intervalos regulares.

Ejemplo de un procedimiento de respaldo en la Empresa X

Procedimiento 7 Respaldo de Aplicaciones.

1. Realizar diariamente la salva de:

a) Sistema Contable (CONTAB).

b) Sistema de Control de Información Clasificada (SCIC).

c) Sistema de Control de componentes (Everest).

d) Sistema de Control de Actualizaciones (WSUS).

e) Sistema de Representación Geoespacial (SIRGE).

Al finalizar la jornada de trabajo en discos compactos en dos versiones. Una copia es guardada en el local del administrador de la red y la otra en la oficina de la secretaria del director.

Responsable: Administradores de sistemas

2. Verificar la integridad de la salva.

Responsable: Administradores de sistemas

3. Consignar en el registro de salvas de aplicaciones (Registro 4) las acciones de respaldo realizadas.

Responsable: Administradores de sistemas

4. Realizar un control trimestral (incluyen revisión del registro), del cumplimiento de este procedimiento.

Responsable: Jefe Departamento de Organización y Supervisión

6.8. Seguridad en Redes

En esta parte del plan se incluyen las acciones a realizar para garantizar la seguridad de las redes y sus servicios, mediante la habilitación de las opciones de seguridad con que cuentan los sistemas operativos y de otras iniciativas dirigidas a lograr la seguridad de los servidores y terminales, el acceso a la información solamente por el personal autorizado y los elementos que permitan el monitoreo y auditoría de los principales eventos.

Se describe la configuración de los componentes de seguridad de las redes y servicios implementados y la instalación de los medios técnicos destinados a establecer una barrera de protección entre las tecnologías de la entidad y las redes externas. Para lo cual se tiene en cuenta:

1. Barreras de protección y su arquitectura.
2. Empleo de Cortafuegos, Sistemas Proxy y otros.
3. Filtrado de paquetes.
4. Herramientas de administración y monitoreo.
5. Habilitación de trazas y subsistemas de auditoría.
6. Establecimiento de alarmas del sistema.
7. Dispositivos de identificación y autenticación de usuarios.
8. Software especial de seguridad.
9. Medios técnicos de prevención y detección de intrusos (IPS/IDS).

Se especifican los procedimientos requeridos para el cumplimiento de las obligaciones de los administradores de redes en relación con la seguridad, en particular los relacionados con:

1. La aplicación de los mecanismos que implementan las políticas de seguridad aprobadas.
2. El análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.
3. El análisis del empleo de los servicios de red implementados.
4. Las acciones de respuesta en caso de la ocurrencia de incidentes o actividades nocivas.

Se incluyen los procedimientos instrumentados para la verificación de la seguridad de las redes y la detección de vulnerabilidades.

Ejemplo de un procedimiento de auditoría de eventos del sistema operativo en la Empresa X

Procedimiento 8 Auditoría de eventos del sistema operativo.

1. Realizar diariamente la revisión y análisis de los registros de los eventos generados por el sistema operativo de la red.
2. Investigar las causas de cualquier anomalía detectada y determinar si se está en presencia de un incidente de seguridad, actúa según lo establecido para esos casos.
3. Emplear, cuando se requiera, el software SAWMILL para la revisión de las trazas de auditoría.
4. Anotar las acciones realizadas y sus resultados en el registro de auditorías de eventos del S.O. (Registro 5).
5. Mantener la disponibilidad y actualización de las herramientas que garantizan la auditoría de los eventos del sistema operativo.

Responsable: Administrador de la red

6. Realizar una verificación trimestral del cumplimiento de este procedimiento.

Responsable: Jefe Departamento de Informática

6.9. Gestión de Incidentes de Seguridad

Se describen las medidas y procedimientos de detección, neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o degraden su funcionamiento, minimizan el impacto negativo de estas sobre la entidad.

Los incidentes de seguridad incluyen entre otros:

1. Acceso (intentos de acceso) no autorizado a un sistema o sus datos.
2. Interrupción no deseada o negación de servicio.
3. Uso no autorizado de un sistema para el procesamiento o almacenamiento de información.
4. Suplantación de identidad.
5. Cambios a las características del equipamiento, las aplicaciones o datos del sistema sin el conocimiento o consentimiento del responsable de dicho sistema.

Al producirse los incidentes es fundamental que existan los mecanismos para:

1. Detectar e identificar eficazmente el incidente.
2. Crear estrategias de mitigación y respuesta.
3. Establecer canales confiables de comunicación.
4. Proporcionar alertas tempranas a quien lo requiera.
5. Ofrecer una respuesta coordinada a los incidentes.

A partir de los resultados obtenidos en el análisis de riesgos, se determinan las acciones a realizar para neutralizar aquellas amenazas que tengan mayor probabilidad de ocurrencia en caso de materializarse, así como para la recuperación de los procesos, servicios o sistemas afectados, precisan en cada caso:

1. Qué acciones se realizan.
2. Quién las realiza.
3. Cómo se realizan.
4. De qué recursos se dispone.

Los procedimientos para la gestión de incidentes especifican los pasos a seguir para garantizar:

1. La correcta evaluación de lo ocurrido.
2. A quién, cómo y cuándo se reportan.
3. Los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial.

Se habilita un registro donde se consignan los incidentes que se produzcan en la entidad, que es conservado por un período no menor de cinco (5) años y es utilizado como criterio de medición para la gestión del sistema de seguridad informática.

Ejemplo de un procedimiento de gestión de incidentes en la Empresa X

Procedimiento 9 Interrupción en las comunicaciones

1. Informar a la Dirección de la Empresa la situación que se ha presentado.
2 Identificar si la interrupción es causada por factores externos o internos.
3. Reportar la interrupción al proveedor del servicio si el problema radica en la línea de comunicación.
4. Restablecer la operación y establecer las causas de la interrupción y determinar posibles acciones para evitar su reiteración una vez solucionado el problema.
5. Anotar las acciones realizadas y sus resultados en el registro de incidencias. (Registro 6).
6. Reportar el incidente a la OSRI.

Responsable: Administrador de la red

7. Anexos del Plan de Seguridad Informática

7.1 Listado nominal de Usuarios con acceso a los servicios de red

Se habilita un listado de usuarios autorizados por cada servicio, especifican nombre, apellidos y cargo que ocupa en la entidad, así como los servicios para los que está autorizado.

7.2 Registros

Se definen los documentos de registro que se determinen a partir de los eventos y procedimientos que demanden dejar constancia, ya sea por requerimientos legales y de supervisión, con fines de análisis para elaborar tendencias o simplemente para el control de las actividades que se realizan, en correspondencia con las necesidades del SGSI implementado.

7.3 Control de Cambios

Se dispone de un modelo donde se registren aquellos cambios que motivan variaciones en el PSI y que por su magnitud no ameritan editar el plan en su totalidad nuevamente. Se incluyen los cambios que se realicen, la fecha, la parte del plan que se modifica, el nombre de la persona que autoriza la modificación y el de la persona que la realiza.